RE-INTEGRATING INFLUENCE AND CYBER OPERATIONS

GRADUATE RESEARCH PROJECT

Dennis J. Krill, Jr., Major, USAF

AFIT/ICW/ENG/11-06

DEPARTMENT OF THE AIR FORCE

AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/ICW/ENG/11-06

RE-INTEGRATING INFLUENCE AND CYBER OPERATIONS

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Dennis J. Krill, Jr., BS, MIS

Major, USAF

June 2011

AFIT/ICW/ENG/11-06

RE-INTEGRATING INFLUENCE AND CYBER OPERATIONS

Dennis J. Krill, Jr., BS, MIS
Major, USAF

Approved:

\\SIGNED\\	2 Jun 2011
Michael R. Grimaila, PhD, CISM, CISSP (Chairman)	Date
\\SIGNED\\	2 Jun 2011
Robert F. Mills, PhD (Member)	Date
\\SIGNED\\	2 Jun 2011
David J. Robinson, Lt Col, PhD (Member)	Date

Abstract

The art of influence operations as a subset to information operations as well as personnel that practice influence operations for the military have been doctrinally removed from conducting cyber operations. With the openness that the military has created to social networking as a tool for soldiers, the fact that many of the greatest cyber espionage tactics involve a form of influence operations tactic, often in the form of social engineering, to gain, maintain and exploit networks. Continued ignorance in this subject area will lead to exploitable vulnerabilities as well as reduce the military capability to utilize potential attack vectors.

This research presents the reasons behind the separation, and a methodology for getting the two independent operational capabilities to re-integrate, and justifies this as the first step towards a Virtual Intelligence, Surveillance, and Reconnaissance (VISR) capability.

Acknowledgements

To my darling and gorgeous wife, whose patience with me during this past year has given me the strength to finish this research.

To my parents, who lived close enough to visit every weekend, but thankfully respected the space. Hopefully we did make it there enough though!

To my advisors and sponsor, who provided the necessary guidance needed to get this research done on time, in scope, and not letting bite off more than I could chew.

To our pets, I know this meant not nearly enough walks, scratches, or romps. I'm sure you'll forgive me though at the next 'steak night'

Table of Contents

List of Figures

List of Tables

RE-INTEGRATING INFLUENCE AND CYBER OPERATIONS

I. Introduction

1.1 Background

The Air Force has grown and morphed through the use of Information Operations (IO). In the early 2000's, the AF Information Warfare Center (AFIWC) in San Antonio, now the 688 Information Operations Wing, was hard at work in formalizing the Air Force's mission involvement with IO. The newly established Cyber Domain, an outgrowth of the early development of IO, is now unfortunately lacking in a significant mission area; Influence Operations. There is a fundamental flaw in the way in which the Air Force is approaching the conduct of cyber operations, which is missing a significant integrated IO effort of conducting joint operations. Specifically, the Air Force needs to consider how to effectively integrate influence operations, in particular the art of Military Information Support Operations (MISO), formerly known as Psychological Operations (PSYOP) and Military Deception (MILDEC) with cyberspace operations.

1.2 Motivation

The establishment of the Cyber Domain and standup of Cyber Operations have had limited incorporation of the art of *Influence Operations*. AFDD 3-12 *Cyber Operations* includes Influence Operations in the fact that it is a fundamental capability supporting the goal of "Cyber Superiority." (Figure 1 Cyberspace Superiority, Note: emphasis added) (United States Air Force, 2010). The definition of what constitutes

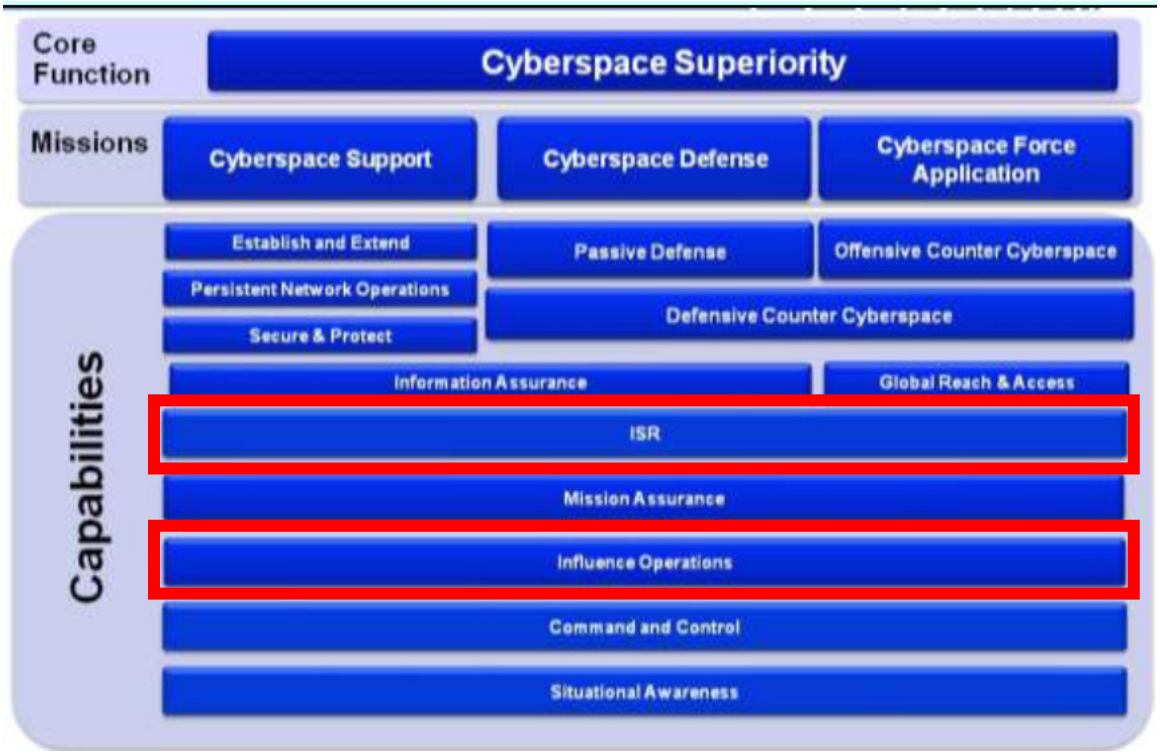


Figure 1 Cyberspace Superiority (United States Air Force, 2010)

Cyber Superiority introduced in this doctrine, defined as "the idea of preventing prohibitive interference to joint forces from opposing forces, which would prevent joint forces from creating their desired effects." (Note: emphasis added) Two issues become evident with this definition, 1) the fact that cyber superiority by definition is reliant on effects based operations (EBO) planning, which is terminology not well received in the joint community (Mattis, 2008) and 2) the concept of truly achieving cyberspace superiority may never be possible. The joint perspective of conducting operations through the cyberspace domain is focused on an integrated IO effort. Each service brings specific capabilities to the fight that must be considered. The transition from a larger IO perspective to the more narrowly focused cyber operations without the use of influence operations has been remiss in training, and continues to develop stove piped mission. A possible reason was to focus cyber operations on strictly handling and manipulating *data*

(i.e. “bits”), not *information,* where information refers to higher level cognitive processing. This research shows that there is a need focus beyond the data itself, but the actual information that this data represents. Influence operations are the critical missing link on how data is interpreted to be information, affecting a person’s knowledge and eventually wisdom.

1.3 Purpose

This research is meant to stimulate thought and hopefully change by demonstrating the disparate ways the military is separating the art of information operations from the practice of cyber warfare, and the need to overcome these divided and compartmented military cultures into a combined force with a common goal. Re-integrating the capabilities of IO will dramatically improve the use of cyber Tactics, Techniques and Procedures (TTPs), in particular, integrating with the crafted arts of influence in order to achieve a desired effect. The first step of this process is in understanding the technology behind cyber operations, which the current methodology in training cyber operations is directed. Secondly, the training must expand to incorporate using cyber capabilities to interlink and manipulate information to human understanding, knowledge, and wisdom and use to our advantage, a monumental step towards the defined Cyber Superiority.

In addition, this work will use integrated influence and cyber operations as a stepping stone to enhance the traditional intelligence, surveillance and reconnaissance (ISR) also shown in Figure 1 as a fundamental capability of Cyber Superiority. The final step is to integrate these operations into an overall concept that can best be described as a

"Virtual Intelligence, Surveillance, and Reconnaissance" (VISR) capability

To accomplish this objective the research will investigate 1) what the art of influence really is, 2) how to apply this in cyber operations, and 3) how to use this understanding to develop fundamental philosophies that can aid intelligence gathering missions using cyberspace.

1.4 Scope

The scope of this research is limiting the discussions to understanding existing organizations primarily in the Air Force, but also some Army, that conduct traditional influence operations activities and cyber activities. The appropriate themes and messages can be integrated outside their traditional delivery mindset, and allow non-traditional cyber operations to be leveraged to achieve the desired effects. Lastly, this research will conclude with a general understanding of how influence and cyber operations are preambles to supporting ISR capabilities that develop the VISR concept.

1.5 Organization

This research is split into six chapters. The first chapter defines the problem statement and scope of the research. The second chapter provides a fundamental historical understanding of influence operations, its missions, and roles as defined by both Joint and Air Force doctrine. Additionally, it introduces cyber operations as defined by the Air Force doctrine, a capability to attack and defend through the use of network operations and electronic warfare. The third chapter begins to analyze the gaps that have developed between influence operations capabilities and cyber operations. It also introduces where opportunities exist that can provide better integration. The fourth

chapter then explains these gaps in terms of deficiencies and solutions using the Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities (DOTMLPF) construct. The fifth chapter and overall endstate of this research is the overall objective of Virtual Intelligence, Surveillance, and Reconnaissance (VISR). Successful implementation of a VISR capability can best be accomplished after influence and cyber operations have integrated, fully enhancing the effects that these capabilities can produce.

Lastly, this research will provide a number of future research options that can be accomplished, some as easy as classroom papers, some more intense for modeling and simulation based on historical use of IO

II. History

2.1 Influence Operations History

``The effective gathering and dissemination of information can constitute an additional, albeit intangible, battle line''

–Sun Tzu *The Art of War* (Sun-tzu & Ames, 1993)

Sun Tzu translates to Master Sun, which has been associated with two prominent Chinese military figures, Sun Wu and a few hundred years later, Sun Pin.(Sun-tzu & Ames, 1993) To add to this confusion, the translations were lost, rediscovered, re-taught, retranslated, and all this done based on new technologies developed over time, thus muddying the waters of Sun Tzu even more.

The confusion regarding Sun Tzu's writings is brought up to illustrate a critical point in regards to influence operations. Puzzling historical writings, misleading vague interpretations, and multiple translations, maybe not intentional, can lead to fundamental military philosophies affectively used throughout the years to instruct strategic thinking. While the data may be static in the scrolls of Sun Tzu, the overall interpretation of the information affecting ones knowledge is the heart of influence operations. Regardless of who or when was the authorship, the translations of Master Sun bear witness to the nearly lost art of warfare, using common sense tactics and techniques found in society of the day to gain advantage over the adversary. In a far removed way, this is what today's military is trying to replicate using Information Operations (IO).

IO as a military concept/term/definition/strategy has been around since the mid 1990's, emanating from earlier coined terms such as command control and

communication countermeasures (C3CM) and Information Warfare (IW). (Jaramillo, 2009) Additionally, the military has used other terms, including irregular warfare (typically Special Ops related), military operations other than war (MOOTW, a term for operations such as humanitarian relief or noncombatant evacuation operations), and more recently non-kinetic operations which is often associated with electronic warfare or computer network operations. Its fundamental foundation has remained fairly consistent as the military began integrating non-kinetic operations into its doctrine and operations planning. This shifted the traditional mindset away from solely using kinetic operations to achieve the desired military effect. Primarily, the use of electronic, network, and influence operations to achieve a commander's objectives emerged as the dominant forces behind non-kinetic operational planning. A byproduct from the information age, the military has for the most part, adapted to include these capabilities to maintain its advantages on the battlefield.

To set an initial baseline, doctrine must be understood as it relates to both influence operations and cyber operations. Joint Publication 3-13, *Information Operations*, is written in to context of a grand Information Environment picture, which is broken down into three dimensions: Physical, Informational, and Cognitive. (Figure 2 Information Environment) (Joint Chiefs of Staff, 2006) The physical dimension constitutes the parts of the environment one can physically manipulate; wires, routers; computers and the overall infrastructure. The cognitive dimension is the knowledge and wisdom of an individual to make decisions. The informational dimension is the interconnection between the two dimensions, where data and information reside.

Joint Publication 3-13 uses the core capabilities, OPSEC, MILDEC, PSYOP, EW,

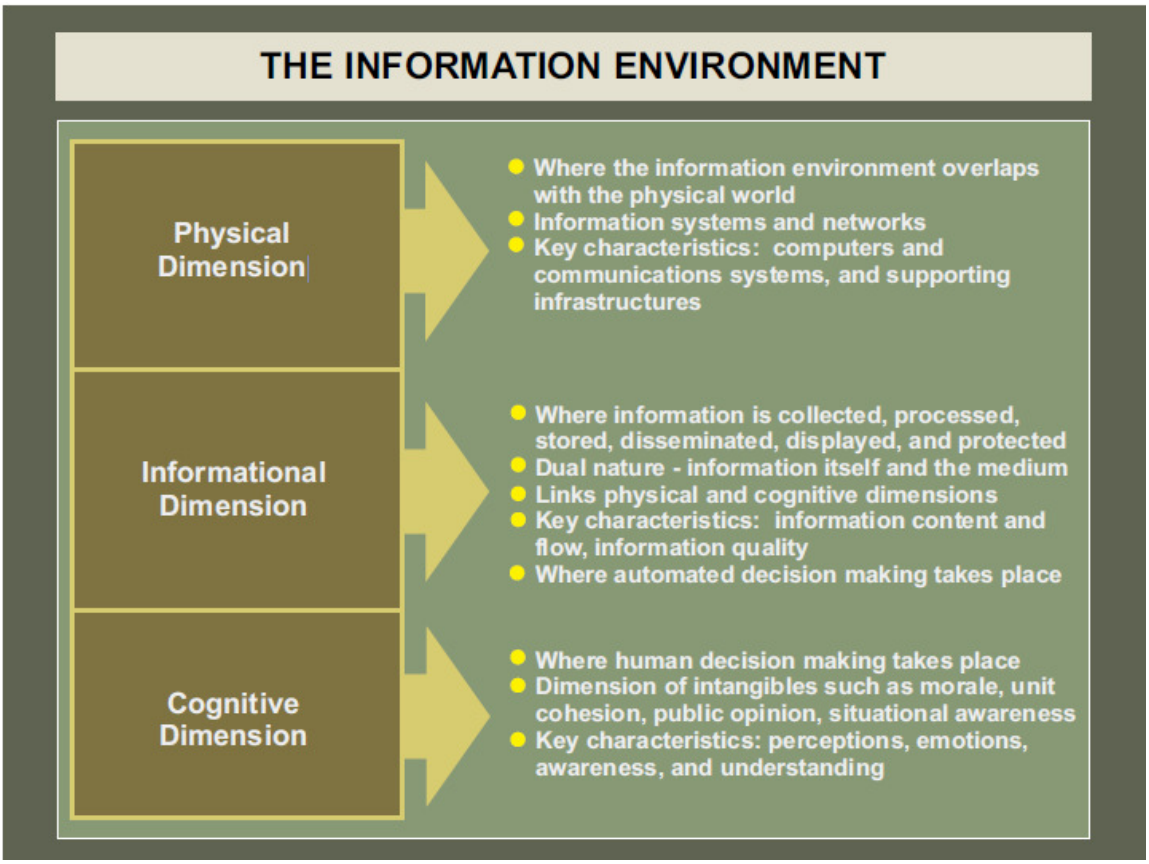


Figure 2 Information Environment (Joint Chiefs of Staff, 2006)

and CNO, for strategic/operational planning. The Air Force merged capabilities of OPSEC, MILDEC, PSYOP to "Influence Operations.", defined (United States Air Force, 2005)

Influence Operations - employment of capabilities to affect behaviors, protect operations, communicate commander's intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander's objectives

- *AFDD 3-13 Information Operations* (United States Air Force, 2005)

In addition to the core capabilities, both Joint publication and Air Force doctrine also incorporated supporting capabilities that include counterintelligence (CI), counterpropaganda, and most importantly Public Affairs (PA). Public Affairs has traditionally been the sole interaction of the military to the global media, but the growth of the military's use of advanced technologies like social networking as well as embedding media in the front lines of operations has dramatically altered the military use of PA.

IO as brought about a dramatic growth in the global media's involvement in reporting military activities to the public, a fusing that the military may not be ready to handle. The initial precedence of embedding of media in warzones during Vietnam Conflict has risen into a real-time war-reporting live, on-air, and streaming across the Internet, straight to the home of the average American. Perceptions and influence, now the conduct of every soldier, sailor, and airman in the heat of battle are now distributed across the world. This is where the military needs to ensure it is properly training its personnel.

2.2 Cyber Operations History

IO is being pushed from a doctrinal standpoint to a more strategic/operational planning mindset. Unfortunately, this is blurring the lines of IO's *network operations* with the new Air Force concept of *cyber operations*, which is a narrowly focused computer network oriented environment. This is developing a counterproductive mentality in the world of cyber operations, perhaps driving towards the conduct of *independent* operations, not *integrated*. The underlying goal of any operations is to bend the mind/will of the target to capitulate to your desire, and cyber operations cannot do

this alone. It is only one tool in a commander's toolbox, and the integration of cyber operations capabilities with other tools is paramount to achieving the desired objectives.

Organizational changes are inevitable in the military, some are dramatic. For example, the establishment of the Joint Functional Component Commands of US Strategic Command to help manage USSTRATCOM's ever growing mission areas. By planting a stake in the ground of an organization, it is the philosophy that that a great tree will emerge reminiscent of the Joseph of Arimathea's "Thorn of Glastonbury."[1] Emotionally, this can be a huge symbolic event, but the reality is a vast majority of military metaphoric stakes are just pieces of dead tree. Few organizational changes have implanted themselves to be mainstays in the military culture; basically the establishment of each service, Army, Navy, Marines, and most recently Air Force, are the only metaphoric trees in the military organization. The commonality between these is the presence of controlling a physical domain. With the establishment of the cyberspace domain, is the next step creating a *Cyber Force*?

At this point it is important to mention the missing physical domain: space. The space domain has a significant role in the history of the cyber domain. Human's first venture into this domain was October 4, 1957, the launch of Sputnik. As a domain, space was first formally recognized in by the Air Force in 2006.

"Space is a domain – like the air, land, sea, and cyberspace – within which military operations take place."

AFDD 3-14 Space Operations (United States Air Force, 2006)

[1] The Thorn of Glastonbury is a legend that Joseph of Arimathea arrived in present day Glastonbury England and planted his staff in the ground on a hill which grew into the original Hawthorn Tree

In comparison to Air, Land, and Sea; Space is now the oldest domain without a formal Department of Defense sanctioned *Space Force*. The Air Force, with the preponderance of assets in space, absorbed the bulk of this domain's mission. The Outer Space Treaty of 1967 ensures every country has equal access to space and has limited Space's full evolution into a contested warfighting domain. The biggest fear was natural phenomenon non-attributable to one nation, phenomena like radiation, rogue particle debris, etc. However, recent events are beginning to demonstrate that this domain and its 40 year old treaties are going to be contested. The Chinese Anti Satellite (ASAT) shoot down on 11 Jan 2007 (National Aeronautics and Space Administration, 2007) and the collision of an operational Iridium communication satellite with a piece of Russian debris (Iannotta & Malik, 2009) are demonstrations that more countries are involved in space and it is not always a peaceful occupation, be it intentional or not. Satellites are becoming smaller and more robust; the difficulty is ever increasing in maintaining space control during a conflict. Reliance of technology in space from GPS to communications is giving countries strategic advantages, and thus being recognized as strategic targets. Not only militarily, but more commercially, this domain has become contested environment with electronic fratricide between bandwidth and frequency command and control capabilities. The development of a Space Force to handle a potential hostile war against space may seem like science fiction, but the aforementioned incidents, this reality may be closer than expected.

Where does this leave the *Cyber Domain*? In many respects the official establishment of a cyber domain within the Air Force has followed a similar path as

space, especially when looking at key organizational players currently handling the warfighting needs of space and cyber. The operational arm of both domains extends from USSTRATCOM (USCYBERCOM and JFCC SPACE) for the Joint element as a sub-unified and component command. The Air Force service component falls under Air Force Space command (AFSPC). The question remains is whether the Air Force has strayed too far from its 'Air Domain' in developing multi-dimensional hybrid air, space and cyberspace personnel.

The reorganization will continue as the use of both space and cyberspace become more of contested warfighting domains. Looking at history, the next logical step may very well be to morph the Air Force back into fighting through only the air domain, while developing a Global Commons Service to handle how the military can fight through space and cyberspace.

III. Analysis of Influence/Cyber Gap

In the previous chapters, historical perspectives from both influence operations and cyber operation were needed in order begin to analyze the missing gaps in capability. This chapter will look at the next step to see the true value of a fully integrated influence and cyber operation.

3.1 Motives behind cyber development

The world has now moved into the advancement of the technical age where people are wired into the internet at all times, almost as a requirement now for some jobs. There is a continuous need for smaller laptops, mobile internet kiosks, smart phone, and maybe eventually entire towns becoming connected wirelessly. People carry more technology in their hip pocket than was ever imagined, capable of the standard web browsing, email, text, and the thousands upon thousands of applications (aka apps) that provide all the news and social networking capability imaginable.

This growth has created an enormous vulnerability, as seen with the multitude of identity theft cases and cyber-bullying the need for computer social connection and acceptance. Our social lives are virtually inter-twined; however the age old issues of youth and adolescence remain. 'Virtual influence' is now affecting real lives. Cyber-bullying conducted by classmates or adults has been attributed to numerous deaths, specifically targeting people with self-esteem issues, and legislation is still playing the catch up game when it comes to use of technology in many of these cases.(www.how-to-stop-bullying.com, 2009)

While these negative connotations of the use of the technology always grabs the news

headlines, it becomes a very sensitive issue when arguing the use of influence operations through the cyber domain for military gain can actually have significant advantages. However, there are still significant advantages and disadvantages that the military must have the forethought to consider, especially when sending young troops into battle. The traditional military always seems steps behind the technology growth relying on intense basic military training to 'toughen up' soldiers, sailors and airmen.

Social networking has a place in the military, be it offense of defensive use, and unfortunately these uses remain largely unexplored. The raid that killed Osama bin Laden is a perfect example on how difficult it is to control. As public released news continues to unfold there are facts that back up some events of the evening of 1 May 2011. This operation was live-blogged near play-by-play over Twitter by a local resident of city, highlighting a potential vulnerability from cyber capabilities. (Cellan-Jones, 2011) Mr. Sohaib Athar, an IT consultant living in Abbottabad, Pakistan, began 'tweeting' the events starting at 1am, not knowing what he was posting until later that night after the official announcement. Some of his posts, including a bit of humor, before realizing what was taking place:

> ***"Helicopter hovering above Abbottabad at 1AM (is a rare event)."***
>
> ***"Go away helicopter – before I take out my giant swatter :-/"***
>
> ***"All silent after the blast, but a friend heard it 6 km away too…the helicopter is gone too."***
>
> ***"Seems like my giant swatter worked !"***
>
> ***"Funny, moving to Abbottabad was part of the 'being safe' strategy"***
>
> ***"What really happened doesn't matter if there is an official story behind it that 99.999% of the world would believe"***

"Osama Bin Laden killed in Abbottabad, Pakistan.: ISI has confirmed it <<Uh oh, there goes the neighborhood :-/"

(Note: ISI=Inter-Services Intelligence out of Pakistan)

"Uh oh, now I'm the guy who liveblogged the Osama raid without knowing it."

- *Sohaib Athar via Twitter* (Athar, 2011)

Two immediate significant issues arise when live social networking reports clandestine events. First, there obviously is the possible tip-off of the events, especially the longer an event goes on. Fortunately, this was a very short-term operation. The second significant issue is, while unconfirmed by conventional media standards, speculation is inevitable as live first-hand accounts of the situation can conflict with official reports. As is the case with this event, Mr. Athar tweeted there was a military presence in the area for up to two hours, but the US only reported the raid lasting 40 minutes. (Cellan-Jones, 2011) These contradictory reports, regardless of substantiating documentation or details, can easily create doubt and the perception of lost trust[2] in the public's eyes.

To further complicate matters, the broadcast media will feed off of these inconsistencies and begins speculative reporting. An example related to the Osama bin Laden raid, Mr. Brian Ross, a reporter for ABC, in a broadcast on the use of a possible stealth helicopter additionally spoke of a possible "Cyber War" associated with the raid that caused electrical and telephone disruption for the exact time period of the raid. (Ross, 2011) If Mr. Ross's speculation is correct, then this is a perfect example of using cyber operations to successfully spear targeted a town for the precise time of execution. Unfortunately even with the helicopter crashing, Mr. Athar's ability to tweet the events still show difficulty of maintaining anonymity to military operations in our interconnected society.

[2] Understanding *trust* is difficult and time consuming to gain, but easily lost

3.2 Influence Operations Gaps

The military has a basic structure in place for conducting specific influence operations, with MILDEC and MISO officers in place. However, an important missing piece with these existing communities continues to be the use of cyber operations. Additionally, this has led to missing out on a greater ability to use influence operations for military advantage to gather intelligence through to the new technology.

One must understand influence operations and how it can be affected through technology as well as the vice, how technology connectivity develops someone's subconscious levels of understanding situations. To put a fictional metaphoric example to the situation, the science fiction film *Inception* created the novel concept that one can affect a belief by moving through many subconscious layers.(Nolan, 2010) In the movie, the target person has engrained beliefs buried deep in the subconscious that can be modified by 'implant' a new belief that changes the overall understanding of a situation, and thus affecting the real world. The plausibility of this is the greater connectivity each person gets to various layers of society, from positive or negative influential persons or media, the more ingrained a belief becomes. The military is playing catch-up to understanding the technology behind what is affecting someone's beliefs. How it can influence people through effective use of MILDEC and MISO using technology is the logical next step.

To understand how one can have the ability to influence someone, an explanation must be made in understanding the inter-relationship between data and information. Simply put, cyber operations can provide *data*, while information operations are responsible, obviously, for *information* and then take this to the next level, influence operations.

3.3 Data vs. Information

> ***Data****... data is raw. It simply exists and has no significance beyond its existence (in and of itself). It can exist in any form, usable or not. It does not have meaning of itself. In computer parlance, a spreadsheet generally starts out by holding data.*
>
> ***Information****... information is data that has been given meaning by way of relational connection. This "meaning" can be useful, but does not have to be. In computer parlance, a relational database makes information from the data stored within it.*
>
> - *Russell Ackoff* (Ackoff, 1989)

In February, 1964, Bob Taylor sat in his Advanced Research Projects Agency (ARPA) office in the Pentagon staring at three computers, each with dedicated connections to single computers around the country (University of California Berkeley, Massachusetts Institute of Technology in Cambridge, and Strategic Air Command). Each computer required different login procedures, different coding, and different technology. Connecting these systems was the goal, and in 1969 the first cross platform communication between the Stanford Research Institute (SRI) and University of California, Los Angeles (UCLA) was a success, transmitting the characters L-O-G-I-N and the rest is history, or the future. (Hafner & Lyon, 1998)

The internet was built around a fundamental philosophy of interlinking information from a user, converting it to data, transporting this data, and lastly converting the data back to information. Computers see data, binary streams of one's and zero's, and interpret this date to machine language, until eventually the machine binary stream to machine code to programming language can be interpreted by human beings. This is still essentially just various levels of data that can be read by only a select few computer specialists capable of interpreting and manipulate this data. The data is now in that gray area where it is actually information to some select highly specialized personnel, but not the masses.

Russell Ackoff's did not stop with defining data and information, but continued to break down a human's mental conversion of data into five categories (Ackoff, 1989):

1. **Data**: symbols
2. **Information**: data that are processed to be useful; provides answers to **"who", "what", "where", and "when"** questions
3. **Knowledge**: application of data and information; answers **"how"** questions
4. **Understanding**: appreciation of **"why"**
5. **Wisdom**: evaluated understanding.

This is the fundamental idea showing how the baseline of the cyber domain is built from the flow of data, and why it is important to incorporate the art of influence, essentially affecting the way someone thinks, learns, understands, and reacts. Gene Bellenger, Durval Castro, and Anthony Mills put together these Ackoff's descriptions into the interrelationship between correctedness and understanding. (Figure 3 Ackoff Interpretation)(Bellinger, Castro, & Mills, 2004) This is an important concept for manipulation reasons, and how using carefully crafted themes and messages can essentially veer the linear line away from wisdom based on correct data to a falsely derived wisdom stemming from incorrect data that shapes different levels of understanding in a situation.

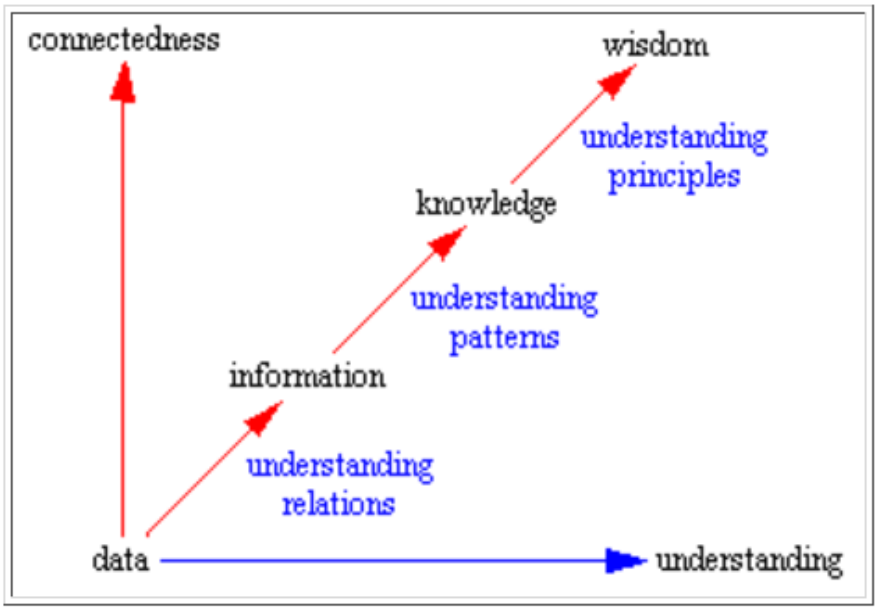


Figure 3 Ackoff Interpretation (Bellinger, Castro, & Mills, 2004)

There is a delicate balance when it comes to the use of technology with the goal of increasing wisdom. As stated, technology primarily lies in the data/information range of the Ackoff graph, not at all part of the knowledge or understanding affected by influence operations. Especially when military decisions depend on a leader making an informed decision based on this growth. Thus, one can look at technology and what cyber can truly provide is only a fundamental understanding of the complexity of the situation. Technology does a remarkable job of inflating the problem though, creating a situation in which the decision maker is thus inundated with excess data, which could easily filter into different interpretations if not properly handled, leading to improper information being pushed to the decision maker. This unfortunately can also be a downside on over-reliance of technology. One can figuratively bury oneself in so much data that useful information is lost.

It is important to grasp the limitations technology places on our decision making. This is why the Ackoff graph is so important. The growth of Correctedness and Understanding on the X and Y-axis are the limiting factors that technology can help or hinder. Technology can be so

"Correct" that it becomes useless, or even damaging. A perfect example is to examine the irrational number for Pi, a number which continues for infinity without repeating. Attempting to calculate Pi using technology will only bog down the processor and potentially lead to crashing the system. However, using a cognitive understanding that there is no solution to irrational numbers, precision in calculation is rounded (for Pi typically rounded to 3.14) something that technology would not fully understand without human programming. At some random, but understandable point, the human mind doesn't 'over think' the situation, and just relies on "Understanding" the situation to round off at the right point to make an informed, but rational decision. This interrelationship is why influence operations are so powerful in conducting cyber operations; the target is not a computer itself, but the user behind the keyboard.

In referring back to Pi example, the human mind is essentially the ultimate technical processor that knows when to "round off" the irrational number. This is the much needed bridge between the information and knowledge in Ackoff's graph. However, without the information filter, the knowledge becomes inaccurate. This essentially leads to the guiding principle to understanding *how* influence operations must integrate into cyber operations.

3.4 Joint Influence Operations, Who has it right?

Each service treats Information Operations and Influence Operations a bit different, primarily because each service has its own culture, methods, capability, and geographic domain(s) to focus activities in. For this reason, it is important to begin by looking at Joint Publication on where Influence Operations actually falls in the grand scheme of strategic warfighting.

Recall from Figure 2 Information Environment that Joint Publication 3-13 describes the Information Environment consisting of three dimensions to operate in and through: physical, informational, and cognitive. (Joint Chiefs of Staff, 2006) On its own, influence operations, is part of the Cognitive Dimension of Joint Doctrine, but with the expansion of influence operations into cyber operations, it can now be looked as interlinking the informational dimension to the cognitive.

Unfortunately, there continues to be service level disconnects on what cyberspace really is, as pointed out by BG Jeffrey G. Smith, Jr. of the Army's Network Enterprise Technology Command:

> ***"There is significant agreement among the services as to the inherent capabilities of cyberpower in the networking, information/knowledge, and people/social domains. There are also currently points of disagreement among the Services as to definitions and taxonomy of cyberspace, including the scope, frameworks, and leadership."*** (Smith Jr., 2009)

The trend for the Air Force is moving away from IO as a capability inherent to service components, but focusing more solely on specific components within IO. The Air Force's focus is on cyber operations and electronic warfare, relying for the most part on the Army to conduct influence operations. General Keith Alexander, dual-hatted as Director of the National Security Agency and Commander of US Cyber Command, said in a 2007 journal article that "the focus of cyber warfare is on using cyberspace (by operating within or thorough it) to **attack personnel**, facilities, or equipment with the intent to **degrading, neutralizing**, or destroying enemy combat capability while protecting our own." (Note: emphasis added) It is understandable the argument he makes regarding IO, and that it can be such a broad category that any action in any domain

can be considered IO from some point of view. However, limiting the Air Force to wanting to "update our doctrine to establish fundamental cyber warfare principles that guide employment of EW and computer network operations forces in support of our national objectives" (Alexander, 2007) is denying the use of influence operations capabilities that can significantly support the ability to *attack personnel,* or *degrade and neutralize capability* focus of cyber warfare.

The Air Force as a service cannot be thought of solely as a delivery platform for IO themes and messages, which is often the case. An example often cited is the use of an EC-130J COMMANDO SOLO to deliver psychological messages through broadcasting television and radio stations. The operators of COMMANDO SOLO certainly are a delivery platform within the *air domain* and are not concerned with the contents of the tape being played. However, this comparison does not translate to *cyber domain*, as access needs to the cyber domain often times require the use of influence operations being pushed to the tactical 'hacker' level.

The Army is most well known as having the prominent MISO functional area expertise for officers, also known as the FA-39 Psychological Operations and Civil Affairs, with in-depth dedicated training. But even senior officers in the Army, the service leaders in training and conducting MISO in direct support of military operations, or during peacetime stability operations, agree that more needs to be done to improve coordination. BG Jeff Smith believes:

> ***"…a future is envisioned in which soft power and the human/social impact of cyberpower is matched together with a hard power that also is transformed by cyber. Smith considers that cognition is the actual goal of military strength, which is at a level above information, which in turn is a level above cyberspace. … His thesis is that Army DOTMLPF is almost only focused on the physical and not enough on the cognitive, which is more important."*** (Zimet & Barry, 2009)

Contrary to the thoughts behind splitting IO capabilities between services, with cyber operations, each service actually provides its own unique cyber capabilities with emphasis in providing support to their own domain. Table 1 Summary of Service Cyber Programs, is a brief summary of each service's independent developments in cyber capabilities and organization. (Zimet & Barry, 2009) This table developed just prior to Cyberspace Command becoming a sub-unified command to USSTRATCOM, and the Air Force cyber element being the establishment of the 24th Air Force. Most important though, the Air Force being the only service that developed a cyberspace concept that excludes the use of integrated information operations capabilities at a service level, solely focused on the network and its architecture. Strangely, this is true despite the 688th IO Wing, home of the 23rd IO Tactics Squadron and 39th IO Training Squadron, subordinate organizations under the 24 AF

Table 1 Summary of Service Cyber Programs (Zimet & Barry, 2009)

Service	Concepts	Architectures	Systems	Organization
USAF	Cyberspace as a Warfighting Domain	C2 Constella-tion	Assurance, Data Integra-tion, GIG	Cyberspace Command
USA	Information and Cognition as a Domain	LandWarNet	FCS, WIN-T, GIG	1st IO Com-mand, NET-COM
USN	IO, NCO	FORCEnet	NMCI, GIG	NETWARCOM
USMC	NCOW	MAGTF-IO	NMCI, GIG	MCSC

NCO = Net-Centric Operations
NCOW = Net-Centric Operations and Warfare
FORCEnet = a portfolio of programs to enable the gathering, processing, transportation, and presentation of actionable information
MAGTF-IO = Marine Air to Ground Task Force-Information Operations
FCS = Future Combat Systems (discontinued in 2009, replaced with Army Brigade Combat Team Modernization Program (Osborn, 2009)
WIN-T = Warfighter Information Network - Tactical
GIG = Global Information Grid
NMCI = Navy/Marine Corp Intranet
NETCOM = Network Command (maintains Army Global Network Enterprise)
NETWARCOM = Network Warfare Command
MCSC = Marine Corp Systems Command

When looking at this table, there is a vast interpretation to how to organize for the use of cyberspace, and how each service interprets the forces needed to support cyberspace. The Air

Force has been at the forefront in the use of cyberspace as a warfighting domain. An undated memo from the Vice Chairman of the Joint Chiefs of Staff shows there is an effort underway at the Joint level to establish the official Joint Terminology Lexicon. While unconfirmed as having actually been signed, this document shows an effort is underway from the Joint Staff level to separate the network operations terminology outlined in IO (computer network attack/defense) with updated terms that incorporate the cyber domain (cyber attack/cyber defense) and clarifies the exploitation aspect of ISR using cyber means. (Cartwright, Undated) The Army, Navy and Marines continue to align their IO forces under the new cyber construct. The way multiple services handle cyber operations is one of the difficult factors in developing joint cyber doctrine.

On 1 October 2010, the Army established its ARCYBER command as the Army component to USCYBERCOM. Officially:

> ***"ARCYBER's mission is to plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army networks. When directed, ARCYBER will conduct cyberspace operations in support of full spectrum operations to ensure U.S. and allied freedom of action in cyberspace, and to deny the same to adversaries."***
>
> (United States Army, 2010) (Note: emphasis added)

While the mission of ARCYBER does not specifically call cyber a domain, however the article does specifically state from an unnamed Army official "The establishment of ARCYBER brings a unity of effort and synchronization of Army Forces operations within the Army cyber domain." Elements of the 1st IO Command, NETCOM (both listed in Table 1), as well as the Intelligence and Security Command (INSCOM) are attached to ARCYBER. The specific elements of the 1st

IO Command that are attached have not been publicly released, leading to questions to what level of IO will be supporting ARCYBER's ability to support "full spectrum operations."

Similar to ARCYBER, the Marine Corps stood up Marine Corps Forces Cyber Command on 21 January 2010 followed a week later by the Navy's Fleet Cyber on 29 January 2010 and allocated 10th Fleet to the mission. (McCombs, 2010)(Fleet Cyber Command/10 Fleet Public Affairs, 2010) . Fleet Cyber and 10th Fleet missions are not unlike ARCYBER, however with the explicit support of naval IO support and integration:

> ***Fleet Cyber Command: direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure and defend the Navy's portion of the Global Information Grid; to deliver integrated cyber, information operations cryptologic and space capabilities; and to deliver global Navy cyber network common cyber operational requirements.***
>
> (United States Navy, 2010) (Note: emphasis added)
>
> ***US 10th Fleet: to serve as the Number Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.***
>
> (United States Navy, 2010) (Note: emphasis added)

In order to try and explain the cyber domain how the services are interpreting this construct, a recent concept attempts to organize complex situations is brought out by Cheripka et al. who propose a definition for Domain to be "a territory or space over which dominion is exercised that is marked by either physical feature or a sphere of knowledge, influence or activity." (Cheripka, Reichart, & Roberts, 2011) This essentially would solidify the need for the art of influence in every established military domain from air, land, sea, space and now cyber. However, there are two points of contention with this article. First, he takes the domain concept too far, by proposing both electromagnetic and information domains. This would only confuse the situation even more-so with overlapping missions along with alienating mission areas even farther from the combined joint fight, rather than integrating mission sets. He proposed the following diagram (Figure 4 Environment vs. Domain) which is slightly inaccurate to the aforementioned Information Environment outlined in Joint Publication.

This leads to the second disagreement point; Joint Publication has the right strategic outlook for looking at Physical, Cognitive, and Information as *Dimensions*. An environment alludes to a more substantive region that can be measured, something of which the Cognitive "Environment" is not always capable. Measuring the reactions, interpretations, and will of a person cannot be done with any form of accuracy.

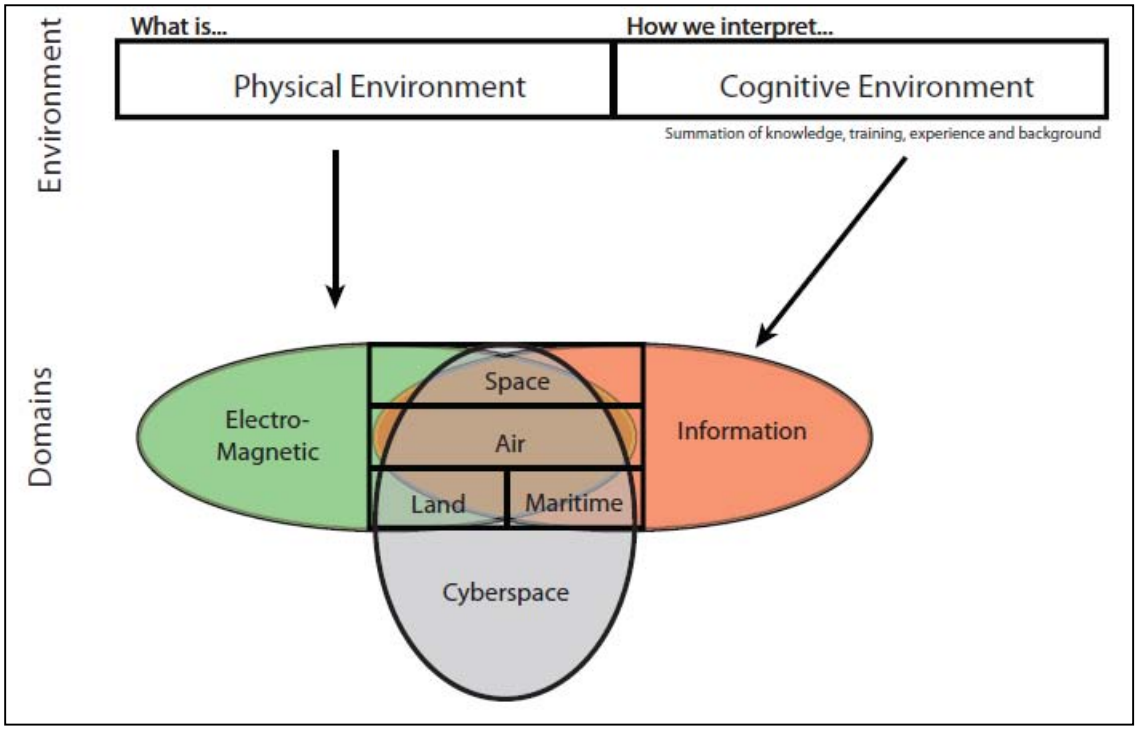


Figure 4 Environment vs. Domain (Cheripka, Reichart, & Roberts, 2011)

A better understanding of the importance of the information environment described in JP 3-13 can be made by identify the vulnerabilities that can be used as targets. In June 2006, Maj Pamela Woolley (Woolley, 2006) developed an early depiction of cyberspace components which closely resembles the current Information Environment model. She initially described cyberspace as three distinct 'domains' (Note: the use of the term 'domain' was still a new concept when this was written). Her domains were represented as physical, cognitive and cyber (digital) (Figure 5 Information Domain).

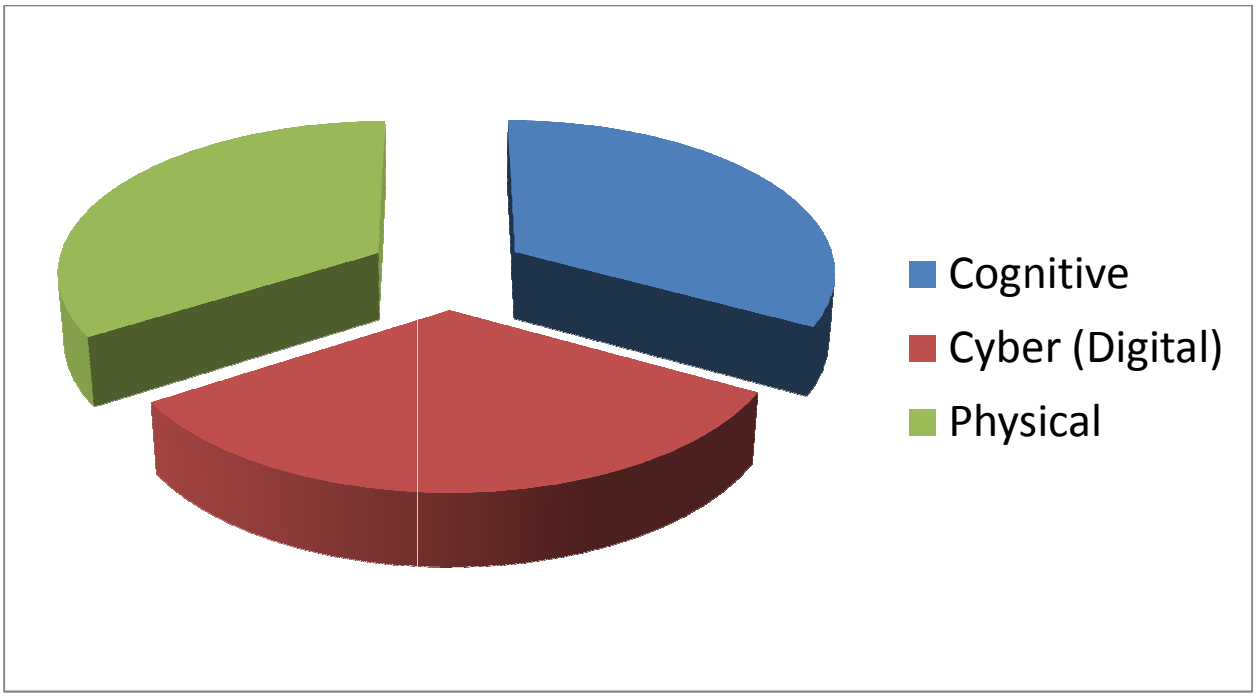
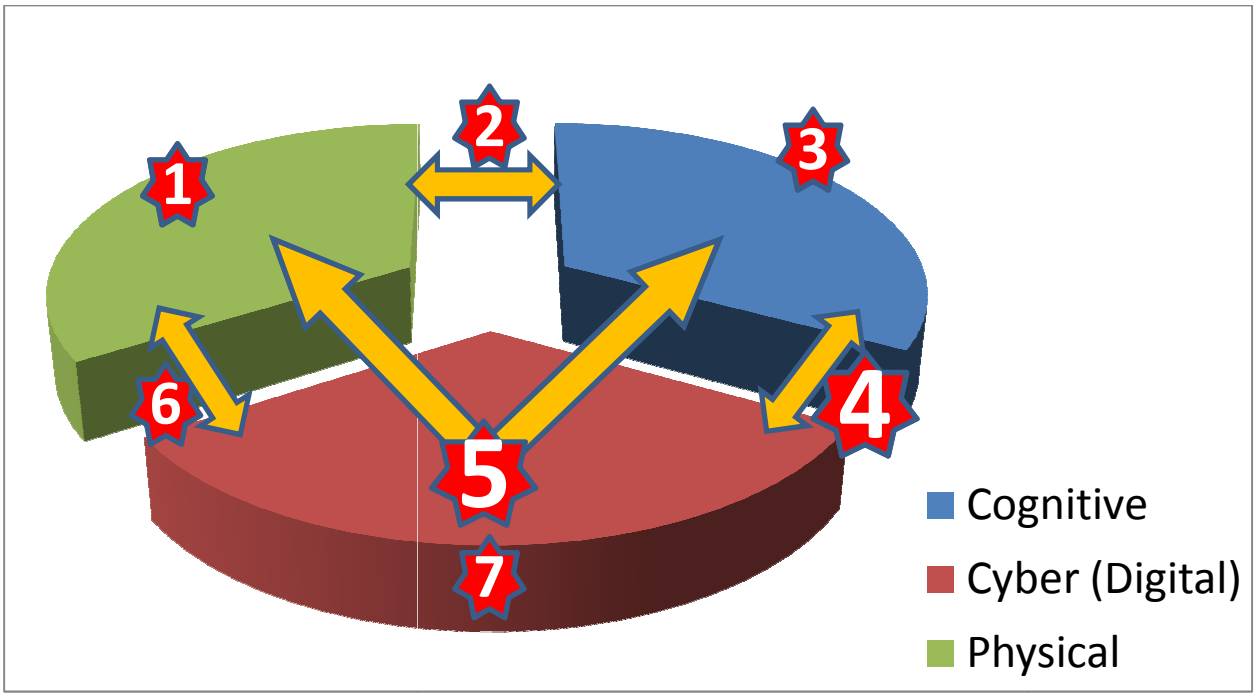


Figure 5 Information Domain (Woolley, 2006)

Using this diagram, she identified the critical vulnerabilities (Figure 6 Information Vulnerabilities) that were important to understanding the boundaries of the cyber domain and where attention needed addressed. In particular, numbers 4 and 5 are the information vulnerabilities that need to be addressed. These constitute the interaction between cyber and cognitive domains.



#4. Interface between cognitive and cyber domains: affecting the transfer of information in/out of cyberspace to the human domain (i.e. the screens, keyboard, etc)

#5. Information transitioning through cyberspace that affects the physical world: Taking control of systems that use cyberspace to control provide the link to control the physical world (i.e. UAV and SCADA systems)

Maj Woolley's initial vulnerability of the interface between cyber and cognitive (#4) was written as a superficial look at human to machine interface disruption. Based on the deeper understanding of what influence operations entails in terms of military operations, the vulnerability actually stems much more involved perspective, getting into the human factors of how a user interacts with a system. Worse yet, is the need to understand how a system interacts

with a person. Beyond the frustrations someone can feel when the "cyber digital domain" fails to respond, but the advent of social networking has expanded the role of this vulnerability, regularly interconnecting our cognitive perceptions to the digital domain.

The information transitioning across cyber from the physical to the cognitive (#5) is unique to cyber. This is what is known as a 'man-in-the-middle' vulnerability where the data/information (depending on how filtered it is) can be modified or denied causing either the cognitive layer to misperceive what is being sent, or the physical layer to react inappropriate to the commands being given.

3.5 Modeling Attempts

In looking at actually modeling this behavior, the cognitive dimension, some organizations have made attempts to some success. In 2003, the Joint Information Operations Warfare Center (JIOWC) out of San Antonio developed with the contractor SAIC a predictive thought outcome model of individual actions based on various inputs, from religious beliefs, social associations, motives and intent, along with many other factors. This effort of Influence Net Modeling, developed for strategic planning, is freeware program called Situation Influence Assessment Module (SIAM) with the latest release in February 2007. (SAIC, 2007) SIAM is "designed to assist people in analyzing complex problems and issues" allowing users to "break down complicated issues into simpler parts, thereby allowing them to recognize and evaluate important relationships among sub-issues more easily." The military goal in this tool is to provide enough details of issues, events, perceptions and other factors to show which were most significant, allowing one to inject themes and messages into the critical nodes affecting a terrorist's Observe Orient Decide Act (OODA)[3] Loop prior to getting to the 'Act' phase. This is

[3] OODA developed from John Boyd's briefing *The Essence of Winning and Losing* Briefing (Boyd, 1995)

a novel concept, but mathematically something that cannot be calculated. The unknown variable of *Free Will* always plays a role, and leaves immense uncertainty in a system designed to minimize uncertainty.

More recently in 2009, Defense Advanced Research Projects Agency (DARPA, the successor of ARPA, inventors of the Internet) is supporting a project to assist soldiers on patrol in Iraq and Afghanistan. A network mapping device known as TRANSTAC (Translation System for Tactical Use) was prototyped by SRI International in California. Army and Marine soldiers would conduct walking patrols to talk with villagers and monitor for unusual activity. Most of their notes were taken using paper notepad and translator, then report back to debrief on what was translated. DARPA saw the need to enhance capability of these patrols by solving a three-fold problem. First was a universal translator that would allow direct interpretation of the translation and playback without the need for the third party. This allows a soldier to focus on the non-verbal communication, an essential piece when it comes to trying to track unusual activity. The second piece of this was in the translation itself. The "DARPA Hard"[4] problem was to understand the various slang and allowing the Western cultural slang to be interpreted in ways that help break the language barrier. A final element of this difficult program was to documenting villager interactions with one another, basically developing a social map that would allow soldiers greater access to information from key villagers, and possible lead to key associations. (Precoda, 2008)

Modeling social interaction remains to be a difficult problem. The concept of uncertainty, free will, and numerous factors in social interaction were explained in an AFIT class

[4] DARPA Hard being the slang term coined by DARPA Program Managers to equate to the most difficult part of the program that needs to be overcome in order to meet each milestone in concept development.

lecture on Management of Information Warfare[5] which discussed a sensitivity analysis to determine what variables are most significant to decision making. The context was in determining how a system manager will react to a cyber attack situation, but the formula is a basic concept that applies to the difficulty in conducting Influence Operations. The basic formula described was:

$$y = f(x_1 x_2 x_3 \ldots x_n) = \mu + \varepsilon$$

An infinite number of variables *x* will lead to an answer μ with a potentially calculable uncertainty error. Unfortunately there is an unknown value that cannot be measured, which is a person's free will (ε) to make independent decisions (aka the 'hunch' or 'gut feeling' factor). Basically, there will always be the human factor in any decision, and the human is the greatest random variable. (Grimaila, 2010)

To further describe the *x* variables, they are an endless list of factors that need to be determined that will affect the final outcome. Factors range from larger issues such as culture, social status, or religion to more specific variables that can't always be measured, for example a person's overall likability or personality. The subjectivity arises in determining the most relevant factors (significant variables), which is what the SIAM model was attempting to organize. These most significant variables have the greater impact to decision making, but are also the most ingrained beliefs that a person may have and the most difficult to influence.

Another important consideration when analyzing the equation is there will never be 100% certainty in a decision. However, this function can be estimated by understanding what was determined to be the most significant factors that would influence a decision. It is important to

[5] Information Warfare is a term used sometimes used for military focused information operations

separate cultural bias and opinions, which may be the most difficult. Looking back to the concept presented earlier with the irrational calculation of Pi, and how influence operations will allow one to round Pi to a degree that is satisfactory to execute an operation. If an operation relies on cyber capabilities alone, then it is possible to lose the proverbial rounding factor which essentially loses the intuitive factors required in order to make an objective decision.

3.6 Social Engineering

The art of social engineering in cyberspace is certainly not something new in everyday society. Most of the greatest civilian cyber criminals relied on social engineering to gain access, including John Draper's (aka Captain Crunch in the hacker community) who used a technique known as 'phone phreaking' to manipulate telephone operators and impersonating touch tones. Kevin Mitnick utilized social manipulation of a society unfamiliar with the inner workings of computers and networks in order to gain initial access. (Lee, 2006). Unfortunately, this is an art that remains unexplored in the military, mostly due to cultural and legal reasons. AFDD 3-12 Cyberspace Operations, states

> ***"The Air force approach to cyberspace operations should address, and remain vigilant of, alternative operating principles and procedures. Some cyberspace users have similar ways and intents of using cyberspace to our own. Other users (possible adversaries) often operate in ways not constrained by our laws or moral values."*** (United States Air Force, 2010)

Many of these techniques used by hackers to gain access are often left out of military cyber doctrine, partly for legal aspects, but more likely because the military moral and ethical codes go against many of the techniques needed to be successful at social engineering. In fact,

both Joint Publication 3-13: *Information Operations* and AFDD 3-12: *Cyberspace Operations* do not mention the use of social engineering as a defensive threat. The previous quote from AFDD 3-12 is the closest reference describing 'alternative operating principles.' Additionally, this document only literally mentions influence operations as it supports Cyber Superiority (Figure 1 Cyberspace Superiority), essentially in the broader information operations campaign effects:

> ***"…the assessment of cyberspace operational effects in support of influence operations requires an in-depth understanding of the warfighter's desired impact on behavior and the ability to measure any resulting behavioral changes."***
>
> (United States Air Force, 2010)

The military honor code engrained into the heads of military cadets that they "will not *lie*, cheat or steal, nor tolerate amongst us anyone who does."(United States Air Force Academy, 2009) Perfectly understandable for a military that must pride itself on upholding its honor, but what does this mean to an officer that is called upon to conduct MILDEC or MISO to support an operations?

For MILDEC, there are restrictions when it comes to lying, basically it cannot be done. A military deception officer is not given any leniency of authority under the Uniform Code of Military Justice to legally lie to a senior officer, if necessary, in order to maintain secrecy of a MILDEC plan. Therefore when training military deception, lying was forbidden which was a limitation, but with a valid work around. The MILDEC courses focused on presentation of forces or information that was truthful, but not the entire truth. The goal was to allow the target audience to draw natural conclusions that would be interpreted inaccurately. Most importantly is to ensure the military deception operation coordinates operations only with the senior officer in

charge, and allow this person to control any questions that may arise from the lower ranking commanders. Conducting a military deception operation is easier said than done, for it only takes one miss-step in conversation, or viewing of abnormal activity, to ruin the deception.

MISO has similar military rules on the use of blatant lying dating back to early days of Psychological Operations. An excerpt from a1979 Army PSYOP Field manual specifically states:

> ***Lying and distortion. Lying is stating as truth that which is contrary to fact. For example, assertions may be lies. This technique will not be used by US personnel. It is presented for use of the analyst of enemy propaganda.***
>
> (United States Army, 1979)

The more recent version of the manual does not explicitly state anything on 'lying', but does outline that one of the purposes of PSYOP is "projecting a favorable image of US actions," which is a often bit difficult to do if you must lie about your actions, especially if discovered.(United States Army, 1993)

The unfortunate truth that needs to be fixed is the same rules that are tying our hands with using social engineering, our being incorporated into bad guy hacker tools that are so easy, designed for 'script kiddies'[6] to use. The user would just download, draft a fake 'lying' email with improper link, and send to anyone, anywhere, and hiding their identity. The Social Engineer Toolkit (SET) written by David Kennedy (aka ReL1K in the hacker community)

[6] Script Kiddie is hacker slang for a user with little fundamental computer understanding, just utilizes simplified graphical user interface (GUI) tools and capabilities built by others without regard to 'how' they work. Typically a user with less regard in the hacker community.

became “a standard tool in (computer) penetration tester’s arsenal.” utilizing most common UNIX based penetration test baselines. (social-engineer.org, 2011)

With social engineering being one of the standard and most prevalent tactics being used against the US military and civilian users, why has the military hand-tied itself to not allow the use of social engineering techniques to be implemented into cyber operations? There continues to be modified group network policies that restrict access and capability and disallow certain activities essentially locking down the network by metaphorically building a stronger castle wall. As they found out in the Greek city of Troy, even the strongest walls can be bypassed with carefully crafted influence techniques, using a deceptive wooden horse. Unfortunately, the long term results from influence operations do not give commanders the results they desire, the immediate feedback of accomplishment. This unfortunately is that double edged sword that was created by the military need for progression and the media’s need to show results.

3.7 The “Sexy Part” of IO

In early 2001, the 92nd Information Warfare Aggressor Squadron in San Antonio was struggling with the concept of conducting its mission of base Multi-Discipline Vulnerability Assessment (MDVA). MDVA’s were using every facet of IO in a 2-week time period to essentially ‘break a base’, find vulnerabilities, physical, network, and on base security, that could be exploited, and then exploit them at the discretion of the base commander. The struggle endured was unfortunately a common theme through various jobs in IO; the art of influence operations would take a back seat to the Network Penetration/Intrusion operations. Influence operations needed much longer than two weeks to exploit, so the resulting briefings were hypothetical examples of what can be done to exploit vulnerabilities. To anonymously quote a

former 92nd commander, “Network Operations is the Sexy Part of IO”. This commander was correct in a way, but for reasons unknown at the time.

The Air Force has always been the lead service attempting to formalize IO. The attempted standup of AFCyber under the 8AF, and the current construct with USCYBERCOM/24AF, the “Sexy Part” as this commander put it, and many other commanders have also migrated to this cyber-only mentality. The integration of influence operations was never realized and often treated as capability beyond the Air Force that didn’t’ produce immediate results that commanders like to see. Sensitive documents being exfiltrated, captured and cracked login/passwords, etc. were immediate tangible results could be shown and fixed. What was not easily understood was what potentially lied underneath the surface of cyber operations. One simple example was the art of password cracking.

Before the increased password policies and CAC login, it was fairly easy to break passwords. The Air Force had fairly relaxed policies in 2001: eight characters, upper, lower, one special character, and non-dictionary. Once the MDVA network team got into a network, they could capture Windows hash files (one-way encrypted files that ‘stored’ Windows login credentials) and let the password cracking tools do their work. The network team would have hundreds of passwords by the time the MDVA was complete. To paraphrase the network team, they would learn the identity of the lonely and disgruntled workers based on deciphering these passwords. Some were various versions of vulgarities, others included base command members. As an influence operations officer, this was something that could be used as an advantage, targeting these personnel as possible insider threats.

Unfortunately, this information was never fully briefed to base commanders during the MDVA outbriefings. MDVA's were conducted as non-attribution, so sharing the information of the names of the 'disgruntled employees were not allowed. Thus, commanders would only be briefed on the first level effects, the ability to get into the networks and crack passwords. As MDVA's became a thing of the past, the focus shifted solely on Network Vulnerability Assessments, continuing to this day. The art of influence becoming irrelevant in the technology age, and this unfortunately could be a mistake that needs remedied.

3.8 Phases of War: Necessary Paradigm Shift

The Joint Publication 3.0 *Joint Operations* depicts the Joint Phasing Model (Figure 7), which shows how the military conducts operations. Long drawn out wars in the Middle East and rising potential threats have shown the warfighting emphasis needs to change to Phase 0: Shaping and Phase IV Stability Operations.

> ***Phase 0: SHAPE: …are designed to assure success by shaping perceptions and influencing the behavior of both adversaries and allies, developing allied and friendly military capabilities for self defense and coalition operations, improving information exchange and intelligence sharing, and providing US forces with peacetime and contingency access. "Shape" phase activities must adapt to a particular theater environment and may be executed in one theater in order to create effects and/or achieve objectives in another.***
>
> ***Phase IV: STABILIZE: …Stability operations are necessary to ensure that the threat (military and/or political) is reduced to a manageable level that can be controlled by the potential civil authority or, in noncombat situations, to ensure that the situation leading to the original crisis does not reoccur or its effects are mitigated.***
>
> (Joint Chiefs of Staff, 2010) (Note: emphasis added)

Phase 0 (explicitly defined) and Phase IV (inherently defined) point to the need to emphasize influence operations in warfare, and leads to the follow next step in developing the Virtual ISR model.

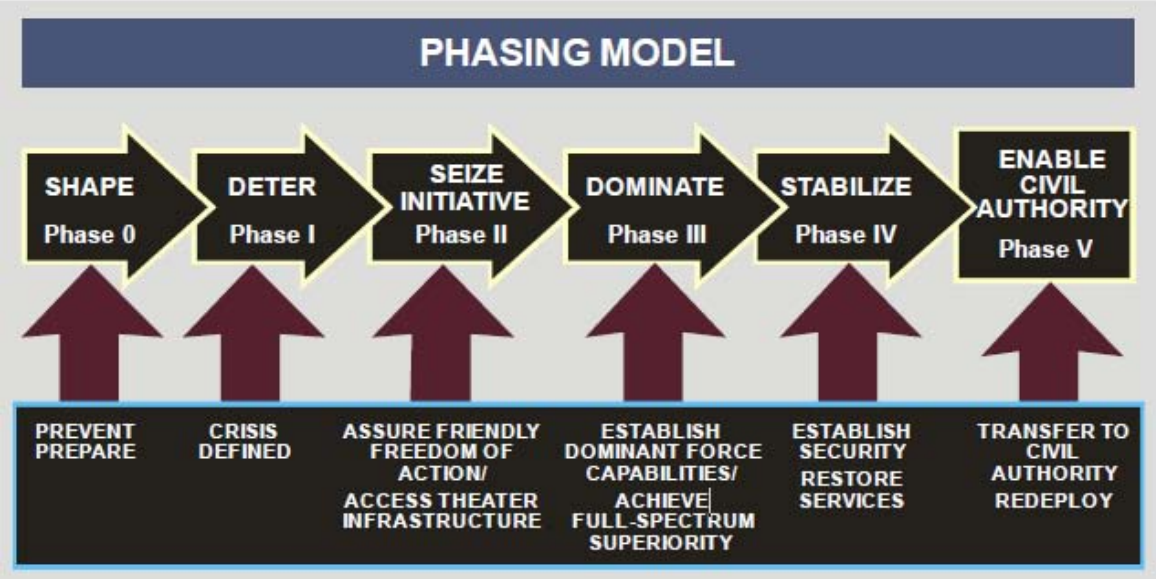


Figure 7 Phasing Model (Joint Chiefs of Staff, 2010)

There needs to be a significant paradigm shift in how the military currently conducts exercises leading up to war. Major theater exercises Austere Challenge in EUCOM to Terminal Fury in PACOM have solely on Phase II and III. For the Air Force, these exercises require certain objectives to be exercised in order to maintain appropriate Air Operations Center accreditation. The ability to conduct influence and cyber operations during these exercises is often notional at best. The military must adapt to the ability to exercise outside the kinetic phases of operations.

To again quote General Keith Alexander "the principal effect of IO is to influence an adversary *not* to take an action, the principal effect of cyber warfare is to deny the enemy freedom of action in cyberspace. Granted by denying enemies' freedom of action in cyberspace, we will also influence them; however, influence is not the intended primary effect-denying freedom of action is the intended primary effect. (Alexander, 2007) General Alexander attempted to eliminate influence operations from cyber by separating the effects, however, in

exploring what effects-based operation are defined as, the need for influence operations even more emphasized.

3.9 Effects-based Modeling Solution

Effects-based Operations (EBO) was a joint concept in military planning to determine really what is trying to achieve and how one can succeed. However, in 2008, Joint Forces Command, then led by Marine Gen James M. Mattis, discontinued sponsoring the terms and concepts related to EBO. (Mattis, 2008) He stated, “Effective immediately, USJFCOM will no longer use, sponsor or export the terms and concepts related to EBO...in our training, doctrine development and support of JPME (Joint Professional Military Education)." Every service except the Air Force soon dropped EBO from its lexicon.

While the other services have pushed EBO aside, Air Force still has EBO as a valid planning capability. This creates a potential conflicting situation in which Air Force cyber operations could plan towards non-approved joint nomenclature, in particular looking at System of System Analysis (SoSA) (Figure 8 System Perspective of the Operational Environment)

Gen Mattis was correct in that EBO planning in kinetic strike and traditional warfare was inadequate and painfully slow to execute. However, he described four ideas relating to EBO would remain in the Joint lexicon:

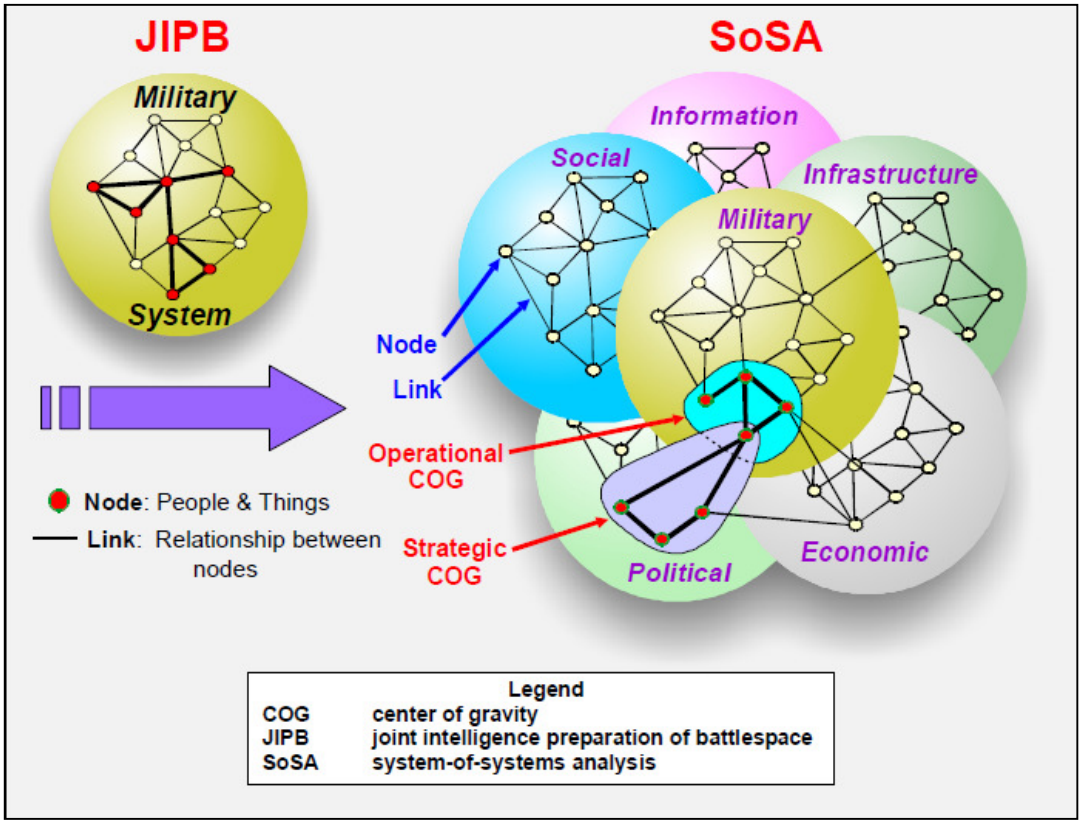


Figure 8 System Perspective of the Operational Environment (Joint Warfighting Center, 2006)

1. Better understanding the history and culture of a society, interaction among military, interagency, and international organizations, socioeconomic makeup, political systems, and other factors in the operational environment.
2. Using mission analysis to visualize and describe commander's intent, thus creating unity of action.
3. Employing nodal analysis as it relates to targeting.
4. Conducting periodic assessments of operations to determine progress

An argument can be made that while EBO as it relates to kinetic planning may be ineffective, the non-kinetic interlinking of cyber operations and influence operations capabilities may still be beneficial

In the case of influence operations and where it best be utilized, the effective use of EBO planning concept may truly be the ultimate solution. This research is not about trying to bring the overall riff that EBO caused in the kinetic planning, but to look at some of the key capabilities that EBO used, in particular the nodal analysis used for targeting, in a purely non-kinetic influence and cyber operations environment.

Early influence operations models (like SIAM) were conducted at the height of EBO employment in mid to late 2000's. These models were based on link/node architecture to find most significant targets to influence and how. The point that needed understanding, and was explained before, there will always be the human free will, that led the need for these models to develop confidence factors. Unfortunately, one of the biggest concerns with these models was the span of influence being conducted from strategic thinkers putting these models together, and not connecting to the tactical level personnel trying to execute based on strategic staffing interpretations. Influence operations, in particular MISO, needed a more tactical method of nodal analysis, which is where the DARPA TRANSTAC system came into the picture.

Nodal analysis at the influence level can now be thought of as the following:

- Example Links: informal communication between individuals, social meetings, gatherings, lineage
- Example Nodes: humans, collective 'hives' (groups with common purpose), web forums (common location of opinions), villages

Cyber operations modeling also traditionally developed using the link/node architecture to describe network design.

- Example Links: formal communication, wires, broadcast nets
- Example Nodes: routers, computers, networks

IV. Closing the Gap

4.1 Introduction

For a common frame of reference, this chapter is divided into the traditional construct outlined in CJCSI 3170.01G *Joint Capabilities Integration and Development System* (JCIDS) process of Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities (DOTMLPF). (Joint Chiefs of Staff, 2009) While not directly leading to an acquisition, this organization provides a methodical look at the current limitations within the influence and cyber operations communities, as well as show the important concepts needing addressed for successful transition back into re-integrating influence and cyber operations.

4.2 Doctrine

Both offensive and defensive cyber operations rely on forms of influence operations to succeed. If a cyber operator can convince an adversary, for example, that a computer patch is not necessary, or a malformed patch is indeed necessary, then the operator has essentially opened avenues to conduct effective cyber operations. For this reason, cyber doctrine must include the use of influence operations with cyber operations. Unfortunately, the only doctrine level document is from the Air Force, AFDD 3-12 *Cyber Operations*.

There is currently a significant void in cyber operations doctrine at the joint level, with no "Joint Publication 3-12" in draft.(Joint Chiefs of Staff, 2011) As shown in the previous chapter though, this is understandable, as the Air Force is the only service to currently separate cyber operations from information operations. Currently, Joint Publication 3-13 *Information Operations* differentiates the cyber and influence operations mission areas into the more specific mission areas. The biggest concern is the lack of 'integration' within the influence arts of

MILDEC and PSYOP with computer network attack and defense. Figure 9 Information Operations Integration into Joint Operations (Notional) , taken from Joint Publication 3-13 shows the overall concept of linking IO activities to Informational Environment Dimensions (reference back to Figure 2). (Joint Chiefs of Staff, 2006) The recommendation for improving this document is to include 'Influence' objective into the 'Computer Network Attack' and 'Computer Network Defense" rows. Additionally, the doctrine in and of itself needs to provide an understanding of the different perspectives each service has taken, namely the Air Force, towards implementing cyber operations. Adding an 'Influence' objective will call light at the Joint level to capabilities influence operations can provide in a cyber operation, allowing each service to then develop their own doctrine accordingly based on their capability.

At the service level, for the Air Force in particular, there must be greater emphasis in existing AF cyber doctrine on the importance of influence operations in cyber operations. AFDD 3-13 *Information Operations,* actually does a very good job in spelling out the need for integration across all IO disciplines, not just influence operations and network warfare, but also electronic warfare.

> ***Information operations are not focused on making decision loops work; IO focuses on defending our decision loops and influencing or affecting the adversary's decisions loops. This integration of influence, network warfare, and electronic warfare operations to create effects on OODA loops is the unifying theme of IO.***
>
> - AFDD 3-13 *Information Operations* (United States Air Force, 2005)

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)

Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOFES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOFES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Dsrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure 9 Information Operations Integration into Joint Operations (Notional) (Joint Chiefs of Staff, 2006)

Throughout AFDD 3-12 *Cyber Operations,* there was a failure to recognize the significance of influence operations, and just how much enabling actions in the cognitive dimension can play a role in accomplishing cyber operations. AFDD 3-12, as the first independent cyber operations doctrine, is understandably written with the Air Force's perspective on military use of cyberspace as a separate domain; however a vast majority of this doctrine is written as if it were joint doctrine. With cyber operations as global and throughout each service, the concept of achieving Cyber Superiority (Figure 1) is a joint concept. Likewise, this AFDD lists the principles of war in relation to Joint Cyber Operations. In fact, this service doctrine quite possibly oversteps its service bounds by explicitly stating "Joint cyberspace operations doctrine is under development. Air Force doctrine seeks compatibility and to influence joint doctrine." (United States Air Force, 2010) (Note: emphasis added) With no indication of a Joint Cyber Doctrine development and the idea of a service doctrine explicitly stating that it seeks to influence the joint doctrine is not practical bottom-up approach. The Air Force arguably claims to have a predominance of forces dedicated to cyber operations, but the guidance to conduct these operations must come from the joint community.

The final recommended change, in order to ensure the military maintains its chain of command and understanding the art of influence, the Air Force Doctrine explicitly stating "influencing joint doctrine" must be removed. The Air Force Doctrine will inherently influence joint doctrine without trying to force the Air Force methodology towards cyber operations onto other services.

4.3 Organization

Organization must be addressed in two main areas. First entails understanding the general organization supporting theaters with a global mission. Secondly, the current Air Force

organizations conducting influence operations need to change their mindset to incorporate cyber capabilities.

The standup of the Numbered Air Force (NAF) 24th Air Force in San Antonio presents the beginning of operationalizing the Air Force element of cyber into its own mission set. This organization is loosely based on the construct of the 14th Air Force and the Joint Space Operations Center (JSpOC). Both elements support global missions and are operationally parent to US Strategic Command. US Cyber Command is a sub-unified command under USSTRATCOM. Joint Functional Component Command for Space (JFCC SPACE) is a component command under USSTRATCOM. Both NAFs have AF Space Command (AFSPC) as the Air Force Major Command (MAJCOM) parent administrative control element.

There is significant debate on the organization of these forces as being effective to theater support, but the important piece, that needs accomplished is the successful employment of an integrated influence and cyber operations requires both elements to be located within the same parent organization. Theater planning cells are the most knowledgeable on the current situation at hand, and when would be the best timing to employ a combined operation. Additionally, timing issues will need successfully coordinated from the unit with tactical control of cyber forces in order to further integrate targeted influence cyber effects with theater activities.

The second major issue needing addressed from an organizational perspective, existing constructs that are in place that support various factions of influence operations from all services need closely coordinate with cyber operations capabilities. For example, Air Force military deception at the MAJCOM and often times at the NAF levels have dedicated personnel and funds. Wing level will typically have two personnel, primary and alternate, planning as an

additional duty to their regular work. Unfortunately, regardless of level, the mindset for these organizations is typically based on military deception operation as they relate to supporting aircraft movements in and around a theater. With the newly formed cyber NAF, it is extremely important that their military deception mission be trained for their unique capabilities. Cyber deception may support hiding aircraft signatures, but hiding network intrusion signatures is more along this person's focus. The unique ability for cyber deception operations is moving and/or manipulating data to create alternate information paths, leading to misinterpretation of knowledge and a false wisdom.

PSYOP/MISO has never been a dedicated career field in the Air Force, although nor has any influence operations for that matter. Maj Timothy Franz in his thesis *IO Foundations to Cyberspace Operations: Analysis, Implementation, Concept, and Way-ahead for Network Warfare Forces* describes this very notion of establishing a dedicated influence operation planner career force. (Franz, 2007) Maj Franz outlined the guiding career path development for both officer and enlisted. Most importantly, identifying trained personnel from the beginning would prevent them from getting re-shuffled back into the Air Force.

4.4 Training

Maj Franz's thesis laid much of the groundwork used in developing the current cyber curriculum (the Cyber 200 and 300 level courses) and it is likely some of his thoughts and ideas were included in the development of the cyber career force. The coursework development was unfortunately hindered by the limited scope that cyber operation is defined by the Air Force. Cyber operations are not solely about computer operations. At minimum, there must be an influence operations training module in these cyber courses. Recommend a more tactical look at influence capabilities from deception and MISO at the Cyber 200 course with an emphasis on the

unique capabilities that influence can provide for cyber operations. For Cyber 300, there should be emphasis must be made on the use of cyber capabilities to actually influence target audiences. Social engineering examples can easily be taught. Additionally, the legal limitations of using influence operations in cyberspace must be emphasized by existing legal briefings.

The course curriculum for the Cyber Warfare Masters program and Intermediate Developmental Education (IDE) program needs a course for training to the capabilities of influence operations and how they apply in cyberspace. A significant portion of cyber defense training was to participation in a cyber defense exercise. One portion of this exercise, treated as the 'fun' part, was developing taunts to the attacking forces trying to get through the network, as well as humorous quips at other schools participating in the exercise. In conducting an actual cyber operation, the use of taunts or response to taunts may very well be a legitimate tactic. The military in its current state of training would not be capable of handling this type of influence operation.

Outside AFIT, there are additional training need is to ensure the existing schoolhouses dedicated to training influence operations are including the use of cyber operations. The 39th Information Operations Squadron at Hurlburt Field, Florida is the only Air Force schoolhouse for cyber and IO training. (Lazane, 2009) They teach Operations Security/Military Deception in what is known as a Signatures Management course, and an overall Information Operations Introduction Course (IOIC) aimed towards theater IO officers and enlisted. These courses must include cyber operations capabilities. As both AFIT and the 39 IOS become more synchronized with signatures management and cyber operations, then these two unique schools can begin to exchange ideas to expand curriculum.

The Army has always been the frontrunners to PSYOP/MISO, with the dedicated FA-39 career specialty training. The Army also leads the military with some unique capability in cyber operations. Unfortunately, their currently advertised curriculum is also lacking in including cyber capabilities. The Army has a PSYOP Officer Qualification Course (POQC), where they instruct PSYOP tactics, techniques and procedures and other critical information. (GoArmy.com) Conducting cyber PSYOP needs integrate into this training.

Lastly, there remains Joint training. Training requirements and mechanisms to track graduates of such training courses as the Joint IO Planning Course must be implemented.

4.5 Material

The material needed for influence operations capabilities is already sourced by the military, be it Air Force or Army. This is under the assumption that the courses requiring additional lessons are capable of incorporating this training with the current instructors. Specialty personnel trained and having the experience in the respective capability may need to be funded for proper lesson plan development and instruction.

4.6 Leadership and Education

Significant changes need to be understood from the senior leaders in all services on the importance of incorporating influence into cyber operations. As more soldiers, sailors, airman and marines are 'plugged in', the annual Operations Security training needs updated with potential adversarial influence tactics targeting them. The opening of social networking sites to the armed forces as firmly emplaced a tactic that every airman is indeed a sensor, capable of greater influence throughout the world.

Social networking has sparked influence campaigns in the civilian world. Internet social networking services like Twitter and Facebook have been important tools of communications for protesters in Egypt. Even though Internet service was suspended and phone text messaging was disabled, a work-around was created by the likes of Google to allow protesters to continue to communicate when the Egyptian government enacted its suspensions. Texts and Tweets were conducted through a third party over traditional phone systems. The use of social networking to spread a common cause that influenced the masses essentially led to the end of President Hosni Mubarak's 30-year regime. (Oreskovic, 2011).

Leadership must stay cognizant that the use of social media is a powerful tool to achieving mission success, and carefully plan operations around this capability being in place for both ally and adversary.

4.7 Personnel

The idea of influence operators, for the Air Force needs to be looked at as a valid and capable career path to pursue. Maj Franz described the personnel needs and requirements. Early development would begin with recruiting personnel in the skill of applied psychology, sociology, and marketing. Influence operation planners, according to Maj Franz, would later include cultural immersion in one or two particular theaters, possibly a media posting aimed at honing public communication skills, continuous coursework in organizational behavior, foreign policy, world religions, cultural studies, and the more military focused strategic communications. (Franz, 2007)

There needs to be an actual method in place at the AF Personnel Center to not just identify information operators trained officers and enlisted, but actually keep them in a career

progression associated with IO as a career. The use of prefixes and suffixes in AF Specialty Code (AFSC) identifiers has been attempted in the past, but there has not been any system in place to align personnel according to these prefixes and suffixes. For example, personnel graduating from the IO Introductory Course taught by the 39 IOS, Hurlburt Field, FL, obtain a 'U' prefix in front of their AFSC that identifies them as IO trained. Until an appropriate influence operations career path implemented, the assignment systems need to do identity matches based on these prefixes and suffixes. Trained IO personnel are lost in the masses and the mission is looked at as additional duty.

4.8 Facilities

Assuming no changes are made to the current facility construct, there is adequate capability. Ideally though, there is a physical separation between the 39 IOS training organization located 39 IOS at Hurlburt Field, Florida, and its parent wing, the 688 IOW in San Antonio. Unfortunately, this situation is firmly established with the 39 IOS recently breaking ground on a new facility to expand their cyber and IO training capabilities.

Lastly, with the expansion of the 39 IOS and the previous recommendation to closely coordinate the AFIT Cyber 200/300 training with what the 39 IOS is teaching, a future consideration to move Cyber 200 and 300 to the 39 IOS, allowing AFIT to truly focus on the technical aspects of cyber warfare, to include the IDE cyber warfare program, and let the 39 IOS handle training the career force cyber training.

4.9 Other considerations – Legal

In training, the military has a responsibility to ensure the legal boundaries are taught to all personnel. However, the world of cyber operations is difficult to remain ahead of, especially

with the exponential advancement of technology, but slow legal changes on the use of new capabilities. Unfortunately the legal system and rules that bind us to certain activities will never catch up to the use of technology to influence adversaries. For this reason, legal aspects must be considered to ensure the appropriate hooks are in place allowing cyber operators to conduct missions that can be somewhat contrary to the training they've received from first joining the military training environment. Military personnel must be taught at a minimum that they can be cyber targets, but the abilities need to be there allowing authorized military members to conduct influence operations with the cyber domain.

V. Striving towards Virtual ISR

5.1 Improving integration of Influence and Cyber

Completing fundamental development and training and written guidance is the first step towards re-integrating these mission areas to achieve success. Chapter 4 outlined the specifics of where training environment curriculum needs addressed. Influence concepts are not at all new, as even Master Sun Tzu had forethought into conducting warfare virtually:

> ***The expert in using the military subdues the enemy's forces without going to battle, takes the enemy's walled cities without launching an attack, and crushes the enemy's state without a protracted war.***
>
> –Sun Tzu *The Art of War* (Sun-tzu & Ames, 1993)

Cyber operations may be a new methods and tactics of conducting warfare, but fundamentally, the art of warfare in this domain is no different. Virtual mastery of conducting operations is the key to future success in warfare. Virtual warfare success leads to other factors of success in wartime environments, one of which is the ability to conduct successful Virtual ISR (VISR) operations.

5.2 Effects-Based Operations in a Non-kinetic Environment

To truly understand the "gaps" between IO and cyber operations, one must revert to re-thinking the concept of looking at the non-kinetic aspects of future conflicts with an effects-based approach.

EBO was a concept that had a big push for implementation into every major operation in the early to mid 2000's, but for non-kinetic operations, where effects truly matter, unfortunately got lost in the overexpansion of EBO. IO at the time was the key to making effects-based

operations effective, but the effects-based push quickly spread beyond the growing field of IO. Because every facet of operations was forced into planning with effects in mind, it was proven ineffective and essentially dismissed from joint doctrine. (Mattis, 2008) EBO may very well have been a contributing factor in formalizing the IO concept in the military, especially in theater, while creating dedicating personnel with proper training. Unfortunately, before IO could catch up to the concepts outlined for EBO, the ability to plan effects was removed from the Joint lexicon. Theater IO Planners then had the extremely difficult task to properly integrating into kinetic operations. To make matters worse for IO, theaters often operate by running exercises or crisis action planning, leaving little time for the necessary Phase 0 Shape/Phase IV Stabilize operations planning. (Refer back to Figure 7 Phasing Model)

When EBO is properly planned, then, social interactions, and better fidelity on what cultural affects play into a person's decisions are better understood leading to effective Phase 0 shaping the battlespace. This first step becomes the foundation that is enhanced with influence and cyber operations integration, and leads to the traditional ISR Phase I Deterrence, or in pure non-kinetic terms, develops the VISR capability. Once one understands what can affect the thought processes that go into decision making, then an integrated influence operations to deliver the necessary themes and messages affecting those thought processes will be all the more successful. With the increase in social networks and mobile media, the ability to target persons with custom tailored messages is much easier.

5.3 Modeling Cyber and Influence Operations…is it possible?

Models are built from studying historical examples and following their precedence. For Influence Operations activities, there are significant historical examples that successfully use MISO and MILDEC for Strategic and Operational employment. Three famous examples include

the Left Hook during Desert Storm to trick the Iraqi Royal Guard to defend the Kuwaiti border, the deceptive landing zones prior to Normandy D-day landings, and the Greeks use of the Trojan Horse to defeat Troy's impenetrable walls. With all of these examples, significant planning was needed, studying the adversary, knowing their vulnerabilities, and exploiting those vulnerabilities. The adversary being the changing factor, but the process of determining the vulnerabilities and exploiting them remains unchanged. This is a key consideration when translating the art of influence into the cyber world.

Can a cyber influence model be built? The SIAM is a strategic approach to modeling. Funding ended for this model development in 2008 as it was transitioning to a web-based application known as DecisionNetS. (SAIC, 2007) It was never intended to use as a tactical influence/cyber integration tool. Unfortunately cyber modeling, especially as it relates to military use, is still at the beginning stages. DARPA's concept was the first step in developing a social network model. This gives insight into the critical factors affecting each person, which allows prioritization of resources.

Col Elisabeth Strines identified in the very early establishments of IO in the military the need to exercise social network mapping. (Strines, 2002). Different scenarios led her to this conclusion, one of which was seeing the ability of personal interaction outside the formal chain of command, and how it led to the distinction of subordinates being able to communicate (or not communicate) up and/or down the chain. She identified this as a valuable tool to senior commanders in order to track personnel interactions laterally and vertically.

Most importantly is the actual integration of so called network theory into operations. The Pentagon established the Human Terrain System (HTS) program, embedding scientific

socio-cultural teams inside Army combat teams and divisions, as well as marine combat teams. (United States Army, 2011) This stemmed from manually diagrammed scientific network mapping work conducted throughout OPERATION IRAQI FREEDOM in Iraq interlinking sociology connections within the Saddam Hussein regime eventually led to the key security personnel guarding Saddam in his spider hole (Wilson, 2010) The HTS mission is:

> ***Recruit, train, deploy, and support an embedded operationally focused socio-cultural capability; conduct operationally relevant socio-cultural research and analysis; develop and maintain a socio-cultural knowledge base, in order to enable operation decision-making, enhance operational effectiveness, and preserve the share socio-cultural institutional knowledge.***
>
> (United States Army, 2011)

Basically, the Army is taking the necessary steps to embed influence operations into their ground activity to map the social networks. There needs to be a parallel effort of imbedding influence operations into cyber operations.

5.4 Conclusion

This research focused on a number of issues and considerations when it comes to integrating influence and cyber operations. The capability is certainly needed, and the organizations exist that can do this. The full capability of cyber operations cannot be limited solely to the use of attacking and defending computer networks using the electromagnetic spectrum or digital means. Influence operations exist inherently from an adversarial perspective, using social engineering to target both civilian and government, in order to gain information or access into networks. This understanding needs to be incorporated into the military to use in

both training and operations execution that enable successful defense and counter-attack using both cyber enabled influence tactics, as well as influence enabled cyber tactics. These capabilities will be realized with successful effects-based operations planning either pre-hostility staging (Phase 0) or in planning for stabilization efforts (Phase IV).

VI. Future Research

6.1 Expanding the Virtual ISR concept

ISR operations are conducted a multitude of ways, but continue to rely on traditional collection capabilities to achieve mission success. These traditional methods are narrowly focused and need to be modified to include the increased reliance within the cyber domain. Joint Lexicon appears to be re-defining ISR in terms of cyber operations, but this concept certainly is far from complete. For example, is conducting computer ping sweeps or port scans part of ISR, or the initial phases of cyber operations? Numerous legal factors need to be addressed in this regard, including breaking down the barriers of Title 10 Military Operations and Title 50 Intelligence gathering.

6.2 Cyber Influence Modeling Comparison

This research mentioned only a few capabilities that were developed in cyber modeling, and how influence themes and messages can be integrated. Additionally, there is a number of commercially available social networking software mapping options that could be used to develop a complete cyber influence campaign model. This research would require significant access to the information and themes and messages, the centers of gravity for the campaign, and the outcome to determine if the influence net modeling tool works.

Multiple tools could be considered, from afore mentioned SIAM or DecisionNetS. Additionally, with the opening of social networking on the .mil military domain, there are many possible commercial mapping tools that can be used to track the social networking use in the military. Preliminary research found two possible tools for comparison, NodeXL (CodePlex, 2011) developed for Twitter, Flickr, YouTube as well as local email, or MapMySocial

(MapMySocial, 2011) for Facebook, Twitter, LinkedIn, and Foursquare social networking sites. A comparison study could be conducted in a closed network environment that logs use and creates connections, simulating a military environment.

6.3 Cyber Superiority

The concept of Cyber Superiority was introduced in AFDD 3-12 *Cyber Operations* but this doctrine is focused on the Air Force's philosophy of achieving superiority in a warfighting domain, modeled after Air Superiority. More in-depth analysis of the actual concept of Cyber Superiority is necessary, is it achievable, and what it means to each service. Can cyber superiority truly be obtained in interconnected environments? Comparisons should be conducted on Cyber Superiority with that in other domains: land, sea, air, and space. For example, in contrary to the Cyber Domain, the ability to achieve Space Superiority is much more possible simply due to the high entry cost to access the Space Environment.

6.4 Electronic Warfare (EW) Integration

While influence operations were intentionally left out of doctrine for cyber operations, there continues to be difficulty in defining the role of traditional electronic warfare capabilities and how they integrate into cyber operations.

The Electronic Warfare history is a well established community that has had difficulty establishing itself into the fast pace growth of cyber operations. General Alexander specifically stated "Now is the time to update our doctrine to establish fundamental cyber warfare principles that guide employment of EW and computer network operations forces in support of our national objectives." (Alexander, 2007) Unfortunately, the integration of the art of EW and exploiting

the electromagnetic spectrum are not well defined, nor have some of the proposed integration concepts been well received by the EW community.

The main focus of this topic would be to balance the existing and well established organizations responsible for EW, more defined by constants in the electromagnetic spectrum, with the fast-paced and ever changing growth in cyber warfare. Certain capabilities intertwine (e.g. wireless, cellular data, etc) that require closer consideration on capability exploitation between the two groups of organizations.

Bibliography

Ackoff, R. L. (1989). From Data to Wisdom. *Journal of Applies Systems Analysis, Volume 16* , 3-9.

Alexander, K. B. (2007). Warfighting in Cyberspace. *Joint Forces Quarterly , 3rd Quarter* (46), 58-61.

Athar, S. (2011, May 1). *Twitter*. Retrieved 2011, from ReallyVirtual: mobile.twitter.com/reallyvirtual?max_id=64792874516094978

Bellinger, G., Castro, D., & Mills, A. (2004). *Data, Information, Knowledge, and Wisdom*. (G. Bellinger, Producer) Retrieved 4 11, 2011, from http://www.systems-thinking.org/dikw/dikw.htm

Boyd, J. (1995, Jun 28). The Essence of Winning and Losing. Retrieved 2011, from http://stevenshack.com/johnboyd/assets/essence_of_winning_losing.pdf

Cartwright, J. E. (Undated). Joint Terminology for Cyber Operations.

Cellan-Jones, R. (2011, May 2). *BBC News.* Retrieved 2011, from Bin Laden raid was revealed on Twitter: http://www.bbc.co.uk/new/technology-13257940

Cheripka, R., Reichart, C., & Roberts, K. (2011, March). Operational Environment. *IO Journal* , pp. 23-28.

CodePlex. (2011). *NodeXL*. Retrieved 2011, from NodeXL: Network Overview, Discovery and Exploration for Excel: http://nodexl.codeplex.com

Fleet Cyber Command/10 Fleet Public Affairs. (2010, Jan 29). *www.navy.mil*. Retrieved 2011, from Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet: http://www.navy.mil/search/display.asp?story_id=50954

Franz, T. P. (2007). *IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-ahead for Network Warfare Forces (Limited Release).* Wright Patterson AFB, OH: Department of the Air Force, Air University, Air Force Institute of Technology.

GoArmy.com. (n.d.). Retrieved 2011, from Psychological Operations Officer: http://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/intelligence-and-combat-support/psychological-operations-officer.html

Grimaila, M. (2010, Fall Quarter). IMGT 687 Managment of Information Warfare. *School of Engineering, Air Force Institute of Technology, Wright-Patterson AFB OH* .

Hafner, K., & Lyon, M. (1998). *Where wizards stay up late: The origins of the Internet.* Egully.com.

Iannotta, B., & Malik, T. (2009, Feb 11). *U.S. Satellite Destroyed in Space Collision*. Retrieved from Space.com: http://www.space.com/5542-satellite-destroyed-space-collision.html

Jaramillo, N. K. (2009). Information Operations: Where Has It Gone? *IO Journal , 1* (2), 11-20.

Joint Chiefs of Staff. (2009, Mar 1). *CJCS Directives Library.* Retrieved 2011, from CJCSI 3170.01G Joint Capabilities Integration and Development System Process: http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf

Joint Chiefs of Staff. (2011, Mar 9). *Joint Doctrine Hierarchy.* Retrieved 2011, from http://www.dtic.mil/doctrine/doctrine/status.pdf

Joint Chiefs of Staff. (2010, Mar 22). *Joint Publication 3-0: Joint Operations.* Retrieved 2011

Joint Chiefs of Staff. (2006, February 13). Joint Publication 3-13: Information Operations. *Information Operations* .

Joint Warfighting Center. (2006). *Commander's Handbook for an Effects-Based approach to Joint Operations.* US Joint Forces Command.

Lazane, M. (2009, Sep 1). *Hurlburt Field*. Retrieved 2011, from 39th IOS breaks ground to prepare for cyber-demand future: http://www2.hurlburt.af.mil/news/story.asp?id=123165909

King, M. (Producer), & Lee, R. (Director). (2006). *The History of Hacking* [Motion Picture]. Discovery Channel.

MapMySocial. (2011). *MapMySocial*. Retrieved 2011, from http://www.mapmysocial.com/pages/welcome.xhtml

Mattis, J. N. (2008, Autumn). USJFCOM Commander’s Guidance for Effects-based Operations. *Parameters* , pp. 18-25.

McCombs, A. J. (2010, Jan 28). *Ft. Meade News*. Retrieved 2011, from Marines launch into cyberspace with new command : http://www.ftmeade.army.mil/pages/news/stories/2010/jan/cyber.html

National Aeronautics and Space Administration. (2007, Apr). *Orbital Debris Quarterly News Vol 11 Issue 2.* Retrieved from http://www.orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv11i2.pdf

Thomas, E., Nolan, C. (Producers), & Nolan, C. (Director). (2010). *Inception* [Motion Picture].

Oreskovic, A. (2011, Feb 1). *Reuters*. Retrieved 2011, from Google launches Twitter workaround for Egypt: http://www.reuters.com/article/2011/02/01/us-egypt-protest-google-idUSTRE71005F20110201

Osborn, K. (2009, May 18). *FCS Is Dead; Programs Live On*. Retrieved 2011, from Defense News: http://www.defensenews.com

Precoda, K. (2008, Aug 4). Iraq Communications Translation. (D. J. Jr, Interviewer)

Ross, B. (2011, May 5). *ABC News*. Retrieved 2011, from Seals Used Secret Stealth Helicopter: http://abcnews.go.com/GMA/t/video/seals-worlds-1st-stealth-helicopter-13533840

SAIC. (2007). *Influence Net Modeling for Strategic Planning*. Retrieved 2011, from SIAM: http://www.inet.saic.com/inet-public/

Smith Jr., J. G. (2009). A Unified field Theory for Full-Spectrum Operations: cyberpower and the Cognitive Domain. In L. K. Wentz, C. L. Barry, & S. H. Starr, *Military Perspectives on Cyberpower* (pp. 29-71). Fort Lesley J McNair, Washington DC: National Defense University Center for Technology and National Security Policy.

social-engineer.org. (2011). *Computer Based Social Engineering Tools: Social Engineer Toolkit (SET)*. Retrieved 2011, from The Official Social Engineering Framwork: http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Social_Engineer_Toolkit_%28SET%29

Strines, E. J. (2002). *Social Network Mapping: A New Tool for the Leadership Toolbox.* Alexandria VA: Department of State, The Senior Seminar, Air Force Fellow.

Sun-tzu, & Ames, R. (1993). *Sun-tzu: the art of warfare : the first English translation incorporating the recently discovered Yin-ch□üeh-shan texts.* (R. T. Ames, Ed.) Random House Digital, Inc.

United States Air Force Academy. (2009, Apr 16). *Factsheet: Honor Code*. Retrieved 2011, from http://www.usafa.af.mil/information/factsheets/factsheet.asp?id=9427

United States Air Force. (2010, Jul 15). *Air Force Doctrine Document 3-12.* Retrieved from Cyber Operations: http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf

United States Air Force. (2005, Jan 11). *Air Force Doctrine Document 3-13.* Retrieved from Information Operations: http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-13.pdf

United States Air Force. (2006, 11 27). *Air Force Doctrine Document 3-14.* Retrieved 2011, from Space Operations: http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-14.pdf

United States Army. (2010, Oct 1). *Army Establishes Army Cyber Command*. Retrieved 2011, from http://www.army.mil/-news/2010/10/01/46012-army-establishes-army-cyber-command/

United States Army. (1993, Feb 18). *Field Manual 33-1*. Retrieved 2011, from Psychological Operations: http://www.enlisted.info/field-manuals/fm-33-1-psychological-operations.shtml

United States Army. (1979, Aug 31). *Psychological Operations Field Manual 33-1*. Retrieved 2011, from Free Republic: http://www.freerepublic.com/focus/fr/546409/posts

United States Army. (2011). *The Human Terrain System*. Retrieved 2011, from http://humanterrainsystem.army.mil

United States Navy. (2010, Dec 1). *US Fleet Cyber Command/US 10th Fleet*. Retrieved 2011, from http://www.fcc.navy.mil/

Wilson, C. (2010, Feb 26). *Slate.com.* Retrieved 2011, from Searching for Saddam: Why social network analysis hasn't led us to Osama Bin Laden: http://www.slate.com/id/2245232

Woolley, P. L. (2006). *Defining Cyberspace as a United Stated Air Force Mission.* Wright Patterson AFB, OH: Dept of the Air Force, Air University, Air Force Institute of Technology.

www.how-to-stop-bullying.com. (2009). *How to Stop Bullying*. Retrieved 2011, from Cyber Bullying: http://www.how-to-stop-bullying.com/cyberbullying.html

Zimet, E., & Barry, C. L. (2009). Military Service Cyber Overview. In L. K. Wentz, C. L. Barry, & S. H. Starr, *Military Perspecives on Cyberpower* (pp. 1-27). Fort Lesley J McNair, Washington, DC: National Defense University Center for Technology and National Security Policy.

Vita

Major Dennis 'Jim' Krill is a Cyber Warfare Intermediate Developmental Education Program student at the Air Force Institute of Technology, Air University, Wright-Patterson AFB, Ohio. After completion of this AFIT Program, he will be assigned to HQ USAF/A8XI Strategic Integration. He worked for six years in various Information Operations staff assignments in Lackland AFB TX, Stuttgart Barracks, Germany, and Ramstein AB, Germany that included Red Team leader, military deception instructor, influence operations tactician/planner, and special programs planning. Maj Krill has also worked in space and missile operations; including a missile combat crew commander, missile warning staff officer, and space control planning and theater integration.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
16-06-2011	Graduate Research Project	18 June 2010 – 16 June 2011

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Re-integrating Influence and Cyber Operations	N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S)	**5d. PROJECT NUMBER** N/A
Dennis J. Krill, Jr., Maj, USAF	**5e. TASK NUMBER** N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Institute of Technology Graduate School of Engineering and Management 2950 Hobson Way Wright-Patterson AFB, OH 45433-7765	AFIT/ICW/ENG/11-06
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Mr. Steven C. Landes National Air and Space Intelligence Center (NASIC)/GTRP 4180 Watson Way Wright-Patterson AFB, OH 45433-5648 Comm 937-656-1698 steven.landes@wpafb.af.mil	**10. SPONSOR/MONITOR'S ACRONYM(S)** NASIC/GTRP **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approval for public release; distribution unlimited. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The art of influence operations as a subset to information operations as well as personnel that practice influence operations for the military have been doctrinally removed from conducting cyber operations. With the openness that the military has created to social networking as a tool for soldiers, the fact that many of the greatest cyber espionage tactics involve a form of influence operations tactic, often in the form of social engineering, to gain, maintain and exploit networks. Continued ignorance in this subject area will lead to exploitable vulnerabilities as well as reduce the military capability to utilize potential attack vectors.

This research presents the reasons behind the separation, and a methodology for getting the two independent operational capabilities to re-integrate, and justifies this as the first step towards a Virtual Intelligence, Surveillance, and Reconnaissance (VISR) capability.

15. SUBJECT TERMS

information operations, IO, influence operations, cyber operations, network operations, psychological operations, military information support operations, military deception, intelligence surveillance and reconnaissance

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT	ABSTRACT	c. THIS PAGE			Dr. Michael R. Grimaila
U	U	U	UU	78	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 785-3636 x4800 michael.grimaila@afit.edu